NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

AN EXPERT MODEL FOR AN INTEGRATED
INTELLIGENCE INFORMATION SYSTEM

by

Gary Douglas McLean

March 1989

Thesis Advisor: Tung X. Bui

---

89   6   20   036

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED		1b RESTRICTIVE MARKINGS			
2a. SECURITY CLASSIFICATION AUTHORITY		3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; Distribution is unlimited.			
2b DECLASSIFICATION/DOWNGRADING SCHEDULE					
4. PERFORMING ORGANIZATION REPORT NUMBER(S)		5 MONITORING ORGANIZATION REPORT NUMBER(S)			
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b OFFICE SYMBOL (If applicable) 37	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School			
6c. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000		7b. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000			
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER			
8c. ADDRESS (City, State, and ZIP Code)		10 SOURCE OF FUNDING NUMBERS			
		PROGRAM ELEMENT NO.	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

11. TITLE (Include Security Classification)

AN EXPERT SYSTEM MODEL FOR AN INTEGRATED INTELLIGENCE INFORMATION SYSTEM

12 PERSONAL AUTHOR(S)
McLean, Gary D.

13a. TYPE OF REPORT Master's Thesis	13b TIME COVERED FROM _____ TO _____	14 DATE OF REPORT (Year, Month, Day) March 1989	15 PAGE COUNT 102

16. SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17	COSATI CODES		18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Marine Corps Intelligence, Integrated information system, Expert system, Hypertext, metasystem

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The current Marine Corps tactical intelligence information flow at battalion-level is hierarchal in nature, and structured in design and syntax. It is completed manually using a checklist approach to ensure adequate control of the data flows. This thesis investigates the issues in developing and implementing an automated expert system for collecting and disseminating tactical intelligence, using commercially available systems. Background, system objectives and an Integrated Knowledge Based System and Database Management System structure are discussed. Knowledge acuisition and revision through end-user computing using an off-the-shelf expert system are emphasized. A system requirements review is conducted to stress the need for further development through prototyping.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a NAME OF RESPONSIBLE INDIVIDUAL Tung X. Bui	22b TELEPHONE (Include Area Code) 408-646-2360	22c OFFICE SYMBOL 54Bd

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

i

An Expert System Model for an Integrated
Intelligence Information System

by

Gary Douglas McLean
Captain, United States Marine Corps
B.S., United States Naval Academy, 1980

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

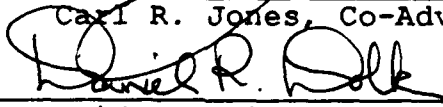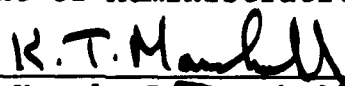from the

NAVAL POSTGRADUATE SCHOOL
March 1989

Author: _____
                Gary Douglas McLean

Approved by: _____
                Tung X. Bui, Thesis Advisor

        _____
                Carl R. Jones, Co-Advisor

        _____
                David R. Whipple, Chairman,
                Department of Administrative Sciences

        _____
                Kneale T. Marshall
                Dean of Information and Policy Sciences

ABSTRACT

The current Marine Corps tactical intelligence information flow at battalion level is hierarchal in nature, and structured in design and syntax. It is completed manually using a checklist approach to ensure adequate control of the data flows. This thesis investigates the issues in developing and implementing an automated expert system for collecting and disseminating tactical intelligence, using commercially available systems. Background, system objectives and an Integrated Knowledge Based System and Database Management System structure are discussed. Knowledge acquisition and revision through end-user computing using an off-the-shelf expert system are emphasized. A system requirements review is conducted to stress the need for further development through prototyping.

Accession For	
NTIS GRA&I	X
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

iii

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

A. BACKGROUND

The ability to collect and organize data into useful information has grown dramatically in the past few years, largely due to technological advances in artificial intelligence applied to expert systems, database management systems and programming techniques. This quantitative leap in capability has made combat information and intelligence potentially available to every Commander and small unit leader who has authorized access and can manipulate the voluminous data. However, to exploit this capability, a means to correlate information so that it can become useful for tactical decision making is required. Essential elements of information must be parsed from the larger body of information, disseminated quickly, and presented in a manner that the user can understand. Additionally, as the user gains more knowledge about the problem and becomes familiar with the system, more detailed information must be made available to him upon request. As more information becomes available in a shorter period, the issue of an integrated information system becomes increasingly important. The author believes

1

research reveals little application of this science has been made at the lower tactical levels of the military in support of the intelligence cycle; that is, collecting, evaluating, processing and disseminating information, for which Artificial Intelligence (AI) technology can be applied.

Governmental sponsorship has spurred enthusiasm in Artificial Intelligence in general, and has generated an avid interest into exploiting AI techniques for future information systems (RADC, 1986, p. 1-2). The potential to enhance current information processing systems with AI techniques is recognized. When the information system contains processes that aid the user in using information through active knowledge processing, it is called an integrated information system. Integrated systems consist of one or more databases managed by a database management system, and a knowledge base and knowledge base system to support deduction, explanation and presentation of information. (RADC, 1986, p. 1-2)

The current tactical intelligence flow is largely hierarchal in nature, and is structured in design and syntax (message formats). Disseminating a piece of information is a function of control and strict adherence to procedures rather than that of timeliness and relevance. Manually passing information between a number of command layers

necessarily carries with it the inherent risk of miscue due to human error.

Additionally, manually collecting and disseminating tactical intelligence is burdensome on the scarce resources of personnel in the Marine Corps. An automated system that can draw correct inferences from voluminous, frequently-changing data, and relay only what is relevant to those Commanders who need it, implies the reduction of staff work and replacement of non-essential personnel. Consider the conceptual model of an integrated, information system comprised of databases, other expert systems, and decision support systems. A system that can tap into those other systems, control those other systems and act as a metasystem, extract pertinent detail, and then pass this information to Commanders on a need-to-know, real-time basis, implies a better, more productive system than is currently in place. Note, however, no tactical decisions are made. In the extreme, only courses of action are presented.

The present methods of performing certain functions within the battalion Combat Operations Center (COC) are extremely labor intensive and costly in terms of opportunity-lost because of the inordinate amount of time spent on recordkeeping, database management, and dissemination. The

sheer volume of message traffic, which requires logging, formatting and transmitting, requires the maintenance (currently by manual methods) of a large, frequently changing database, which takes an enormous portion of the analyst's time. Thus, the analyst is unable to spend more time in qualitative analysis expected of him in addition to his recordkeeping tasks. This, in turn, affects the recipients of the message traffic. Procedures are closely adhered to in an attempt to ensure message traffic arrives at the intended destinations. The process handles messages on a first in, last out priority, without regard to message content. Optimizing the processes of evaluation and dissemination would result in the availability of more accurate and pertinent information in a more timely manner. Automation of the repetitive, structured tasks of the analyst will provide the means to ensure current message and situation databases, efficient and timely dissemination of critical information contained within messages, and an extensive and effective knowledge base to aid the analyst in his decision-making.

Consider an automated tactical intelligence information system that can fully perform the duties of the infantry battalion Intelligence Officer with respect to collecting information from the line companies, sensor input and other

4

collection agencies; then evaluate the content for intelligence value, analyze the intelligence, and disseminate to designated units only that information which is pertinent to them. Such a task is very complex in that it relies on the abilities of the Intelligence Officer. Yet, it is a largely structured environment in which the task is accomplished. By carefully evaluating the content of the received messages from the collection agency, or source, further conclusions are reached based on the facts contained within the messages and facts already stored in a database.

B. SCOPE

The focus of this thesis is a system requirements review of an integrated information system that automates those tasks of the Intelligence Officer and messengers/radio operators in the battalion COC, and provides intelligence to Commanders down to company level. Research is specifically intended to model a system that will extract facts from databases, query an expert system using those facts, and then combine all gathered facts, rules and conclusions together to arrive at a goal intended to either: (1) provide tactical intelligence to those who request it, (2) disseminate information contained in messages to those who require it, (3) add and subtract rules and facts within the database and knowledge base.

5

Research will cover both the expert system methodologies and a database architecture which are appropriate in designing an integrated intelligence expert system, to include the techniques that can be employed in the metasystem.

C. THESIS OBJECTIVES

1. Determine the system requirements for an integrated information system that:

- receives and stores incoming messages,

- detects critical information within incoming messages,

- disseminates information to appropriate recipients,

- provides on-line queries for intelligence for users

2. Demonstrate the potential of computers to aid company Battalion Commanders to send and receive messages.

3. Highlight problem areas development implementing such a system for use in a combat organization.

4. Determine the feasibility of the application of Artificial Intelligence techniques to the automation of certain intelligence functions and message dissemination within the battalion COC.

D. RESEARCH QUESTIONS

1. Identify the system requirements for an integrated information system. Functional areas identified include the

6

metasystem knowledge base and discussion of interconnectivity with a cooperating knowledge base and a database.

2. What are the appropriate limits of the domain that the system should be expected to possess; that is, who should be the users of the system?

3. Can a single system be built that can effectively and efficiently perform message handling capabilities and capture the role of the intelligence analyst with respect to low level information evaluation, to such a degree that automation can be implemented to significantly aid the Commander, the analyst, and company commands?

4. Where are the design issues to be addressed in modelling the proposed system?

E. LITERATURE REVIEW AND METHODOLOGY

Knowledge acquisition obtained for background theory was gathered primarily from government contracts and academic publications. The doctrinal and operational knowledge was gained from doctrinal publications and through interviews of Intelligence Specialists and officers from the First Marine Division. The model design has been heuristic.

F. SUMMARY OF FINDINGS

1. Intelligence Specialists presently cannot complete all their required tasks given the demands placed upon them and the constraints under which they operate.

2. Eliminating the reliance on radio operators in sending and receiving messages is the focus of concern for the intended users of the proposed system.

3. An integrated system is capable of performing all database management tasks, audit-trailing, and communications transmission and retrieval.

4. An integrated information system of this scope requires an incremental approach to implementation. A prototype is necessary in an early stage of development to ensure users requirements are fulfilled.

5. Each battalion has its own standard operating procedures which are unique to that unit. The appropriateness of an expert system in a combat environment and using untested technology with essentially computer-untrained personnel will require further effort.

G. ORGANIZATION OF THE STUDY

This thesis is organized into four major sections, excluding the introduction and conclusions. Marine Corps intelligence considerations provides the background as to why

8

an automated system is needed, and what it should accomplish, from the operational viewpoint of an infantry battalion. The mindset is that the needs of combat dictates the use of technology. The scope of the thesis remains narrow, confined to the needs of the Company Commanders, Battalion Intelligence Specialists, and the Operations Officer of the Battalion. The second major section explains the technology applied within the system. The integrated information system functional areas and design considerations are presented. The third section lists the systems requirements. This, of course, is the basis for the application of the technology mapped onto the problem as presented in the previous two sections. It should provide the reader with an understanding as to how the model will appear. The fourth major section builds upon primarily the last, but utilizes all the preceding sections data to diagrammatically present a system model. Conclusions are drawn and recommendations for further model refinement are presented, along with some of the implications of implementation of this system.

II. MARINE CORPS INTELLIGENCE CONSIDERATIONS

A. GENERAL

This chapter presents the problem definition for this thesis. Information containing the organization of the Marine Corps, functions of the intelligence cycle, and duties and responsibilities of the Intelligence Officer are presented first. The operation of a battalion combat operations center (COC) is explained from the perspective of the Intelligence Specialist. A limited amount of information is included to allow the thesis effort to remain focused and give the reader a better understanding of the scope and complexity of the problem area, and the requirements that the solutions must contain.

B. INTELLIGENCE CYCLE

An understanding of the intelligence cycle is crucial to determining what the system seeks to do in aiding Intelligence Specialists and Commanders. Marine Corps doctrine explains intelligence in terms of four phases that are cyclic in nature. This, then, is translated into the intelligence cycle that provides the framework for the integrated information system.

The intelligence cycle consists of directing, collecting, processing and disseminating (FMFM 2-1, 1980, P. 3-2) intelligence.

1. **Collection**

Collection refers to obtaining data from any source. Retrieval of intelligence, then, is the focus for collecting information. Information is retrieved from collection agencies by means of tactical reports. Information may or may not arrive simultaneously. It may not even be pertinent, or it may only be partially useful. Accurate and timely retrieval of information is the first function of the intelligence component that must be performed.

"Infantry units collect information because of its combat role of closing with the enemy. Infantry may fight to obtain information, or any information by scouting and patrolling...." (FMFM 2-1, 1980, p. 5-9) Information is furnished to the intelligence section within the COC concerning enemy strength, disposition, location, identification, attitude and fighting capabilities. First-hand, up-to-date information on the characteristics of the area of operations is then provided to the field units. The close relationship between the field units and Intelligence Officer is evident: The Intelligence Officer retrieves

collected information from field units via reports. He must then process these newfound facts and may be called upon to draw inferences or pass some of these facts to other interested agencies.

2. Processing

Processing consists of converting information into intelligence and is broken down into the following steps:

"a. Recording information systematically for ease of study and comparison.

b. Evaluating information as to pertinence, reliability of source, and accuracy.

c. Analyzing information is isolate significant elements with respect to the mission and the operations of the command.

d. Integrating information to combine elements isolated in analysis with other known information to form a logical picture of hypothesis of enemy activities which might influence the mission of the command.

e. Interpreting information to form logical conclusions which can serve as a basis for determining the effects on the current intelligence estimate." (FMFM 2-1, 1980, p. 7-1)

The purpose of recording is twofold: (1) Facilitate further processing and dissemination, and (2) provide a record of events for further study and analysis (FMFM 2-1, 1980, p. 7-1). Information is captured on the enemy situation map, the intelligence journal, intelligence worksheets and other like media.

When evaluating information, the Intelligence Officer determines its pertinence and accuracy. Evaluation is accomplished concurrently with recording. Information which is not pertinent is not processed further (FMFM 2-1, 1980, p.7-6). Urgent information is disseminated immediately to those agencies who have a real-time need for it. Accuracy is a function of source reliability and historical consistency. It is dependent upon the Intelligence Officer's experience and biases, for he singularly determines accuracy based on logic and interpretation. Also, as a result of the necessity for information to be passed through echelons of command to the Intelligence Officer, severe degradation of intelligence evaluation can occur. The information is then useless.

After evaluating information and determining whether there is a need to immediately notify others who may need it, the Intelligence Officer refines his evaluation through analysis. "Analysis is the sifting and sorting of evaluated

13

information to isolate significant elements with respect to the mission and operations of the command." (FMFM 2-1, 1980, p. 7-8) Clearly, analysis requires expertise. A thorough knowledge of the enemy situation and principles of military operations is required. An exhaustive analysis can only be completed by referring to the appropriate references that detail enemy order of battle and situation. Additionally, recent experience vis-a-vis a historical base is referenced to obtain present intentions.

The analysis of the incoming information is integrated with other known information to form a logical picture of hypothesis of enemy activities and other influences (FMFM 2-1, 1980, p. 7-8) on the mission. Integration at battalion level is limited to available resources (usually publications and messages/notes from higher headquarters) and the level of expertise of the Intelligence Officer. Expanding his knowledge base of how and where to obtain additional facts increases his integration capability and results in significantly better judgmental interpretations of the information. The Intelligence Officer at this level can access databases/knowledge bases only when he knows where to look, what to look for, and the references/sources are at his disposal. "Points of indecision frequently arise when

individuals lack information, when they overlook what they do know, when they cannot locate information they need, and when they are unclear about particular issues." (Nunamaker, et al., 1988, p. 26) Therefore, omission and commission errors from biases occur in his database.

Processing information then, as long as the tasks remain clearly defined and are narrow in scope, can be automated. The issues of processing are timeliness, accuracy, and relevance. The tasks of processing; that is, recording, evaluating, analyzing, integrating, and interpreting, are largely structured. They are based on a clearly, albeit complex and uniquely defined set of rules. Capturing these rules in an expert system appears to be technologically feasible. The proposed system must integrate the defined functions of the intelligence activities. It must perform the same operations as the Intelligence Officer, but with better answers in shorter time and with greater consistency.

3. Dissemination

The last phase discussed is dissemination. Dissemination is the conveyance of intelligence in suitable form to agencies needing it. There are four principle requirements for dissemination:

15

- Timeliness,

- Usability of form,

- Pertinence,

- Security (FMFM 2-1, 1980, p. 8-1).

a. *Timeliness*

Certain items of information must be given to the affected unit(s) in time so they can adequately react. The immediate significance of such information, such as the case of an impending air attack is obvious. (FMFM 2-1, 1980, p. 8-1) There may not be time enough to complete processing prior to dissemination. A situation evaluated as an urgency must be handled with extreme speed and efficiency. However, the urgency of the situation must first be recognized.

b. *Usability of Form*

Intelligence must be in a form which is easily understandable to the recipient. There can be no margin for misinterpretation/misunderstanding of the content of the communicated information. "Urgent information and intelligence should be disseminated in the form of brief messages, devoid of any nonessential details, to permit its prompt understanding and use by the recipient." (FMFM 2-1, 1980, p. 8-1)

c. *Pertinence*

Units should not receive information for which they have no use. Additionally, useful information should only be received as needed. The doctrinal guideline states that dissemination downward should be selective, based upon the usefulness of the information to the intended recipient (FMFM 2-1, 1980, p. 8-2). Nearly all intelligence should be disseminated upward (FMFM 2-1, 1980, p. 8-2). Here an inherent weakness surfaces with the present mode of information dissemination. Unnecessarily long delays in communicating urgent information can result if the affected units are outside the immediate chain of command of the collection agency. There may exist a need to expeditiously pass combat information from the collector to the user, bypassing normal chain of command channels (FMFM 2-1, 1980, p. 8-2). Currently, unneeded information is passed with the useful intelligence due to the rigid structure of message formats. An automated system can react faster and with greater efficiency that can multiple layers of command involvement that adhere to standard message formats with all lines filled in and passed. Threshold criteria to determine usefulness of information is structured to a large degree.

d. Security

Security is one of the most important considerations in developing any tactical system that conveys information. Disclosure of certain information, albeit unintentional or unknown, to the enemy may render the intelligence (and further intelligence efforts) useless. However, urgent tactical messages of local significance may be sent in the clear (FMFM 2-1, 1980, p. 8-2).

C. SYSTEM DOMAIN

With this doctrinal model defined, the system domain is specified. It must be limited to a narrow scope in order for an expert system to be implemented. Therefore, only standardized messages will be represented; passed from a lower level to a higher level, and to an adjacent, or peer level. This model works for any and all intelligence collected in the manner discussed. Applying it to other more complex tasks of the battalion Intelligence Officer is possible insofar as those tasks are structured. However, for the purpose of this prototype, discussion in these areas will be limited to black-box references.

The expert system developed must emulate the intelligence cycle model shown. System simplicity and flexibility is attained through modularization and independence of duties

18

that the system provides. The brain of the system is the metasystem, described in detail in a later section, which serves as the "traffic-controller". Incoming information is collected and evaluated. Based on this immediate evaluation, several options are available to the metasystem: (1) Information immediately passed on to those units requiring it. Information of this type is limited to urgent and time considerations over-rule other needs, (2) Information is processed in detail. Analysis, integration and interpretation are performed by a module not considered as the metasystem. The intelligence is then passed back to the metasystem for dissemination, (3) Information is discarded as not pertinent, (4) The system determines that the incoming information does not logically couple with its historical knowledge base and database. It would be necessary for the operator to control further action from this point. The metasystem passes control to a module specifically built to handle the options available upon evaluation. If it is necessary to immediately pass the information to units who have an urgent need for it, the module determines who needs it and the metasystem sends it. Likewise, if the information is to be analyzed, then that module takes control. Each module is partitioned so that each is independent of the information in another module to the

19

maximum extent possible. If a module needs more information, it solicits additional information from that module only as needed. The metasystem is responsible for determining where next to send the information based upon the content of that information.

D. ORGANIZATION OF THE MARINE INFANTRY BATTALION COC

A Marine Infantry Battalion is organized into line companies and a headquarters and service company, plus attachments as necessary. The line companies perform the actual combat duties as assigned by battalion headquarters. Headquarters consists of the Commanding Officer (CO) and his staff, which assist him in leading the battalion.

The CO of the battalion controls and commands his combat units primarily through the operation of a command post. The command post is called the battalion combat operations center, or COC. Though the exact organization and placement of personnel within the COC may vary from command to command, all COCs normally house at least the Operations Officer, the Fire Support Coordinator and the Intelligence Officer as principle staff officers. Information provided to the Commander by the staff includes information concerning the friendly situation, plotted on a map or overlay; information on the enemy situation, plotted on a different overlay; and information

concerning fire support and targeting on yet another overlay. Information on these status boards are updated as frequently as the situation dictates and time allows. The Intelligence Officer's specific duties and responsibilities are outlined in the following section. All processing is accomplished by manual methods; an incoming message is received, recorded, logged, and passed on to all the major agencies, including the Watch Officer within the COC for further processing. Each agency then logs the message (each in a separate log) and takes action as appropriate, documenting their action taken. Among the staff agencies who take action is the intelligence section, headed by the Intelligence Officer. He is responsible for directing certain intelligence activities. In order to perform some of his duties, he relies on facts, reported in the form of standardized messages, from line companies and other collection agencies.

E. DUTIES OF THE INTELLIGENCE OFFICER.

The Intelligence Officer advises and assists the commanding officer. In so doing, he is responsible for directing the following intelligence activities:

"(a) The direction, collection, production, and dissemination of detailed, accurate and timely combat intelligence required by members of the command to arrive at

decisions, conduct planning, execute maneuvers, and avoid surprised.

(b) The direction, collection, production, and dissemination of intelligence as directed by higher headquarters.

(c) The direction, collection, production, and dissemination of intelligence to other interested Commanders consistent with the operational requirements of the command." (FMFM 2-1, 1980, p. 1-2)

Note that collecting and disseminating are command points within each activity. Further refinement of specifying the Intelligence Officer's specific responsibilities indicates he produces intelligence by processing data into useful information. In using this information and subsequently delivering the final product of intelligence, he must: (1) estimate the effects of terrain and weather (and other factors) on friendly and enemy courses of action, (2) estimate enemy capabilities and vulnerabilities, including the courses of action he is most likely to adopt, (3) prepare studies and reports for the enemy order of battle and enemy weapons, tactics, techniques, and equipment (FMFM 2-1,1980, p. 1-33).

Many of the battalion Intelligence Officer's tasks are performed within a COC. He must keep the Commanding Officer,

staff, and other interested agencies informed of the characteristics of the objective area and the enemy situation. He completes his responsibilities with the aid of a number of enlisted marines who serve as radio operators, messengers and Intelligence Specialists.

The Intelligence Specialists perform all the record-keeping tasks, audit trails, and database management duties. In the absence of the Intelligence Officer, they are called upon to offer conclusions or state facts on the enemy's capabilities and situation. They manually maintain sufficient documentation in the form of the intelligence journal, workbook, and other notes, to perform their duties. Information maintained in the intelligence journal includes:

- time in (journal)

- file (for audit purposes)

- date-time-group of message

- description

- action taken, available choices are map, staff, troops, (file)

Additionally, the intelligence workbook contains the same information, except in greater detail and it includes enemy order of battle and enemy action. All messages are entered into the journal and everything is always filed for auditing purposes. Over a 12-hour period of a tactical exercise, an

23

estimated 50-75 messages may arrive for action by the intelligence section within the COC. It is important to remember that the intelligence section is also responsible for the enemy situation plot and for providing the Commander and other staff members intelligence concerning the enemy situation.

III. FOUNDATION FOR INTEGRATED INFORMATION SYSTEM

A. BACKGROUND

This chapter discusses the concepts of a knowledge based system (KBS) and the concept of a particular type of database management system (DBMS), and their integration. Within the confines of a KBS the metasystem concept is explained, which is an intended focus of this thesis.

Critical complexities exist in the design and development of integrated information systems possessing knowledge processing abilities. In-place systems have evolved through the consolidation of existing technology (RADC 86, 1986, p. 1-3). Knowledge representation and processing concepts have been integrated with capabilities from database management. Key to integration is the intended use of that system. The issue is determining what technology will drive the system: Will it be a DBMS with knowledge processing capabilities, or will it be a KBS with a database management scheme? The approach of this thesis asserts that the expert system will be the vehicle for information decisionmaking, problem solving, and normal user interface; and that the database management system is the vehicle for data manipulation,

storage, retrieval, and security. To invoke the database manager, the end-user informs the KBS to perform the command. The KBS metasystem (defined later) passes control of the system to the DBMS, until a specified command is called, which of course, re-invokes the KBS. It is the metasystem, then that drives this integrated information system.

B. INTEGRATION ISSUE

The integration of a KBS and DBMS is a combining of their respective design and implementation elements and features into a single functional unit (RADC 86, 1986, p. 5-4). This definition uncovers the concern for the KBS to be able to use the DBMS, or the DBMS to use the knowledge base effectively. Does integration imply that the rule-base must exist within the database? This design integration consideration is only one example of many questions raised by the term "structural unity" of the definition.

An alternative approach is to address functional unity. Allow the KBS to import the DBMS implementation (for this system) but retain system control within the KBS. Is this true integration, or merely an interface issue? It is beyond the scope of this thesis to examine the issue of true structural integration: the issue of this system is functionality. Therefore, functional unity is assumed to

26

fulfill the requirements to label this proposed system an integrated information system.

C. KBS

Traditional programming techniques lack the necessary flexibility to deal efficiently with incomplete information and multiple solutions (ULTRA, 1987). Knowledge-based systems were designed to solve problems which are abstract and substantially more difficult (RADC 86, 1986, p. 2-6). KBSs infer, compare, combine and reason (RADC 86, 1986, p. 2-11) to make decisions for which it was intended. The most important goal for an expert system is to attain the high level of performance that the human expert achieves in that task (Hayes-Roth, Waterman, and Lenat, 1983, p. 43). Expert systems must successfully solve the problems for which they are designed to solve. To be successful, the way in which the correct answer is reached is important. Blindly searching through large numbers of hypotheses should be avoided; instead, the KBS should have the ability to recognize patterns and jump quickly to reasonable conclusions (Hayes-Roth, et al., 1983, p. 44). This section discusses the application of expert system methodologies for the KBS-module of the integrated information system. Further, analysis is limited to the meta-rules of the KBS.

27

An expert system is a computer program that captures the expertise of one or more experts in some domain and applies this knowledge to make useful inferences (Hayes-Roth, et al., 1983, p. 168). Moreover, it has a number of characteristics:

- It applies expert rules in an efficient manner in order to reach acceptable solutions.

- It bases its reasoning process on symbol manipulation.

- Basic principles of the domain reside within the knowledge-base. It must be capable of reasoning about its own knowledge and also of reconstructing inference paths for explanation and justification.

- It must be able to re-formulate the problem (Hayes-Roth, et al., 1983, pp. 169-171). To reformat the problem, it must be able to infer new facts from what it has already been told.

The knowledge-based system is compartmentalized according to the specific function for which it is intended. Each compartmentalized section is comprised of the rules intended to accomplish its calls of tasks, all interconnected and controlled by the metasystem. The compartmentalized knowledge base (exclusive of the metasystem) performs the following tasks:

- Check each incoming message for consistency. Consistency is measured in terms of context (message type) and content. The information in each message is represented by objects that are checked to see if indeed that object can exist in the manner expressed.

- Check each accepted message object for urgency. If the object is regarded as life-threatening or time-critical, then appropriate rules are engaged to take further action.

28

- Route each message. Rules check each object and appropriately disseminate those objects to intended recipients.

- Provide solutions to user-queries.

Expert system methodologies applied to these functions will not be explored further.

D. METASYSTEM

The metasystem is the focal point of this thesis and performs the important tasks of providing strategies about selecting rules, conflict resolution, and parameter passing between compartmentalized rules and external databases. Supplying knowledge about the knowledge in the system improves the performance of that system. The metasystem contains reliable by time-varying data and knowledge, and is likely to have a relatively small solution space. The prescriptive methodologies to be applied to these requirements may include exhaustive search techniques, monotonic reasoning and state-triggered expectations (Hayes-Roth et al., 1983, p.91).

In a metasystem, the application domain is the system itself. The rules about rules are metarules and the inferencing process is metareasoning (Zytkow and Erickson, 1987, pp. 115-121). To perform metareasoning, it follows that the knowledge in the knowledge base must describe the system

in terms of meta representation. This metaknowledge is the information metarules provide (Hayes-Roth et al., 1983, p. 22).

It is difficult, and perhaps not necessary for humans to remain abreast of everything that is happening internally within the system, and to concentrate on performing their intuitive tasks. The metasystem is designed to remain abreast of everything that is happening internally within the system. The program itself must document, justify, modify and understand itself (Hayes-Roth et al., 1983, p. 221).

To be robust, the metasystem must be capable of performing certain functions:

- Select rules. There are several compartmentalized rule-bases which need to be called upon. There must exist rules that determine when to call upon those rules.

- Resolve conflicts. Where more than one rule can be appropriately applied, and the resulting hypotheses differ, there is conflict. Choosing among the many rules that may be relevant at any given moment requires additional rules.

- Maintain facts about the system. Metarules cannot function unless record-keeping of previously used rules, and the new facts that they may have generated, are maintained. Data from this record-keeping is called empirically obtained resource data.

- Justify rules. A complete trace of the line of reasoning may be appropriate in complex decision-making scenarios.

- Detect bugs in rules. Rules that have conclusions that can never be met (syntactic errors), or hypotheses that are not realistic (semantic errors) can be detected by the metarules.

- Provides for program design. Descriptive metaknowledge on interrelations that should exist in the knowledge are used to provide semantic checks of newly acquired knowledge it may have generated. The metaknowledge shows how rules interrelate.

- Justifies program architecture. Users may ask why one rule was picked over another, or why a rule was not considered at all. Having an expert system handle these types of queries calls for knowledge about the consistency, completeness and magnitude of the knowledge, the size and composition of the search space, and other systemic parameters.

- Aid the system to perform better. Metarules can exist to allow the system to reconfigure itself in response to experience.

- Model the program's abilities. The metarules instruct the program about its limitations and appropriate functions. Metarules ensure that the program does not provide solutions for problems it is not capable of answering. (Hayes-Roth et al., 1983, pp. 223-234)

E. DBMS

It is beyond the scope of this thesis to present a comprehensive DBMS overview for implementation within the integrated information system. A separate, complete requirement's analysis concerning database management is required. However, to appreciate the fundamental requirements of the system's database scheme and understand the complexity of the use of integration of the database with the KBS, a discussion of a potential database management system is briefly discussed.

A database management system is a collection of interrelated data and a set of programs to access that data. (Korth and Silbershatz, 1986, p. 16) Its primary goal is to provide an environment that is both convenient and efficient to use in retrieving and storing information to the database itself. In pursuance of this goal, it should provide users with an abstract view of the data. That is, the details of how the data is stored and maintained is hidden. To be convenient and efficient, a DBMS used in this system model should focus on the end-user and the capabilities it should contribute to the integrated information system. Three important issues to be addressed are: power, presenting information in a way that is useful to the users, and performance. Selecting an appropriate DBMS to score high on these points is important for the successful exploitation of the potential of an integrated system. Traditional database systems, albeit powerful, flexible and perhaps user-friendly, lack an important precept that must be a driving force for those who seek information while in combat: speed and ease of data retrieval coupled with its contribution to the power of the integrated system.

The system should not dictate, due to its limitations, how it will present the data on the screen. Instead, all

users, even those who are not sure what answer(s) they are looking for, should be guided though the information quickly, viewing only what is essential in a form they are most comfortable with. Without comparison of traditional databases, a new database scheme is offered: Hypertext. With the assumption that all system components should be "off-the-shelf" nondevelopmental systems, a hypertext system may be a solution for field use, intended to operate with a cooperative KBS.

Hypertext is a DBMS that allows you to connect nodes of information using associative links (Fiderio, 1988, p. 238). It mimics a person's ability to access information quickly and intuitively by reference. Information is parsed into small, syntactically discrete units called nodes, which consist of a single concept or idea. Links are used to connect the nodes. By embedding them in text or by separate reference, you are connected to associated or ancillary information. Links, then, are the mode of transportation in a hypertext network. (Fiderio, 1988, pp. 238-249) They can help define the node's relationship to other nodes within the database, clarify graphics or give greater detail of explanation.

By design, hypertext is a browsing, or perusing tool. Its power lies in the links. A graphical browser (Fiderio, 1988, p. 240) allows you to skip through the database and move directly to an area you are interested in, even though you may not know exactly what you are looking for. A viewing filter (Fiderio, 1988, p. 240) suppresses detail and allows the user to view only that which he desires. Virtual structures change dynamically when you add or delete nodes and links, depending on their description. Virtual structures are similar to relational database views (Fiderio, 1988, p. 244). Links can be generated by text parsers or by user-definition. For example, a parsed message with one of its objects being POSITION, places the association between the nodes UNIT and POSITION. Further, if the unit is an antitank unit, an associative link would be placed between ANTITANK_UNIT, UNIT, and POSITION.

The DBMS will be called upon in three instances:

- The owner of the database, the Intelligence Specialist, makes changes to one of the databases he has privileges to modify.

- Users of the database request information from the DBMS. Based on the request code, the system lets the user query the DBMS direct for information he is authorized to have. A Platoon Commander, in reading for a patrol, may wish to have a real-time update on terrain and weather, known enemy positions in his area, and other pertinent facts. By using a query-construction window (Begeman and Conklin, 1988, p. 262), the DBMS searches for the detail of data this platoon command would likely desire. For

34

example, a Platoon Commander is not likely to want to view division-level data. Additionally, embedded links would let the Platoon Commander know if there is additional or related information. By highlighting the text with cursor movement, the Platoon Commander retrieves additional information in the detail he desires.

- The system's knowledge-bases call upon the databases for facts to use with their rules. All incoming messages must first be checked for consistency and urgency. Consistency checks ensure data integrity and concurrency within the database, as well as eliminating redundancy. For example, an instance of message object TIME would be checked to see: (1) if that message is timely. A message, even though just sent, that contains a suspect TIME would potentially disrupt data updates; (2) if the additional information is plausible. The TIME instance of this would be message checked against another time or time-interval or other known facts; (3) if that TIME instance could be the TIME instance of a duplicate message, sent by another unit, with the same information.

To perform these routine checks, the rules concerning consistency and urgency are called upon, and the metasystem system calls upon the database manager to provide those rules with the knowledge, or facts stored in the database.

F. ORGANIZATIONAL STRUCTURES.

The organization of the KBS and the data structure of the DBMS must not only be compatible, but cooperative to the extent that it combines to form a robust system. Similar organization structures facilities integration and allow the domain expert to directly interface with both systems with minimal confusion.

The KBS should be object oriented such as with Neuron Data's NEXPERT, an expert systemshell. In it, an object has a name and belongs to a class. It is a discrete unit which consists of a single concept or idea, and has a series of properties that describe its qualities. It also has subobjects which constitute its components. For each class, object and subobjects, relations are defined. With such a structure, the real-world can be represented with the hierarchical descriptions. The KBS, then, can reason at the class level, object level, or component (subobject) level.

The DBMS should be likewise organized; that is, similarly organized. Hypertext nodes correspond to the objects of the KBS. Hypertext links correspond to the objects' properties of the KBS. However, it is the node-object similarity that is important. Similar organization can lead to a fuller, more robust integration.

IV. DEVELOPMENT OF THE SYSTEM MODEL

A. INTRODUCTION

The tactical intelligence integrated information system's required capabilities can be implemented using seven major functional areas. These functional areas, with the exception of the database manager and security, are the major components of the KBS. Within each of these components, it is the metasystem that provides the links between each functional area. The Intelligence Specialist (operator) Interface provides the man-machine interface. The Intelligence Specialist is the "owner" of the system, and the interface allows the owner to control the KBS, or intervene in any of the functions of the KBS. The Security functional area provides the rules within the KBS that delineate those further system actions (by external routines or programs) that are taken in the event that the KBS or DBMS has detected unauthorized intrusion. Security in this sense is limited to the data and knowledge security of the DBMS and KBS. A more detailed discussion of computer security issues are contained in Appendix A. The Message Receive and Filter functional component receives incoming messages in standard

37

tactical message format from a system user. A system user in this context is an authorized system addressee who can send and receive messages, and read from the database only; as opposed to the system owner, who controls the KBS through the Operator Interface. System users are the Unit Commanders and those personnel that communicate with the system and system owner (Intelligence Specialist). After the Message Receive and Filter receives the entire message text, each line is parsed into message objects and evaluated for information validity (consistency), timeliness, and content- or time-urgency. Further, the message is filtered or categorized into a request (query the system) or a certain message-type. The Request Management functional component allows the system owner and users to gain access to the DBMS, based on the request code. It also logs all queries to the DBMS and KBS. The Message Routing functional area contains the rules and knowledge bases that determine what addressees get certain message objects, and in what priority. The Database Manager functional area is the actual integrated DBMS(s) of the KBS. The system owner or users will leave the KBS and the DBMS will fully control operations within that area. The subject of integrated DBMS and KBS, however, is a topic for further research. The Message Format Translator is the final

functional area of the KBS before an external routine or program transmits the message or request response. The message formatting rules customized pertinent message objects into a standard tactical message format, attaches the addressee(s) and priority (if urgent) and calls the external routine to send the message or request response.

The functional area interconnectivity presents the overall system concept of this thesis. Each functional area is separated and discussed individually in terms of its functional low, state-transition diagram, and a summary to gain a better understanding of the requirements of the system.

The functional area interconnectivity diagram shows the complete system concept in a black-bow representation. Each functional area is presented individually, showing the inputs and outputs on its functional flow analysis diagram (Figure 1). The state diagrams represent the possible state the functional areas can be in as a result of the metasystem control.

B. FUNCTIONAL FLOW ANALYSIS AND SUMMARY BY FUNCTIONAL AREA

1. Intelligence Specialist Interface

The Intelligence Specialist Interface serves as the operator control for the KBS (see Figure 2). By intervening in the automatic processes, the operator retains the ultimate

control of all system functions, for it is important to keep the analyst in the decision loop at all times. Decisions not to perform certain actions with information which may ultimately affect lives and resources shall appropriately remain the responsibility of the command and his staff (Ultra Systems, 1987).

The purpose of the interface between the expert system and the intelligence specialist is to control the operation of all functional areas of the system through the interaction with the expert system shell, and be provided with updated information on a real-time basis, of all knowledge contained in the knowledge bases. The State-transition Diagram (Figure 3), represents the possible states that the Operator Interface functional area can be in.

Through this interface with the KBS, the operator can process control actions from operator input. He can perform read and write privileges to the enemy situation database, the friendly situation database, and the addressee database. He has read-only privileges from the message-log and request-log databases: these two databases provide the audit trail of every transaction of the messages.
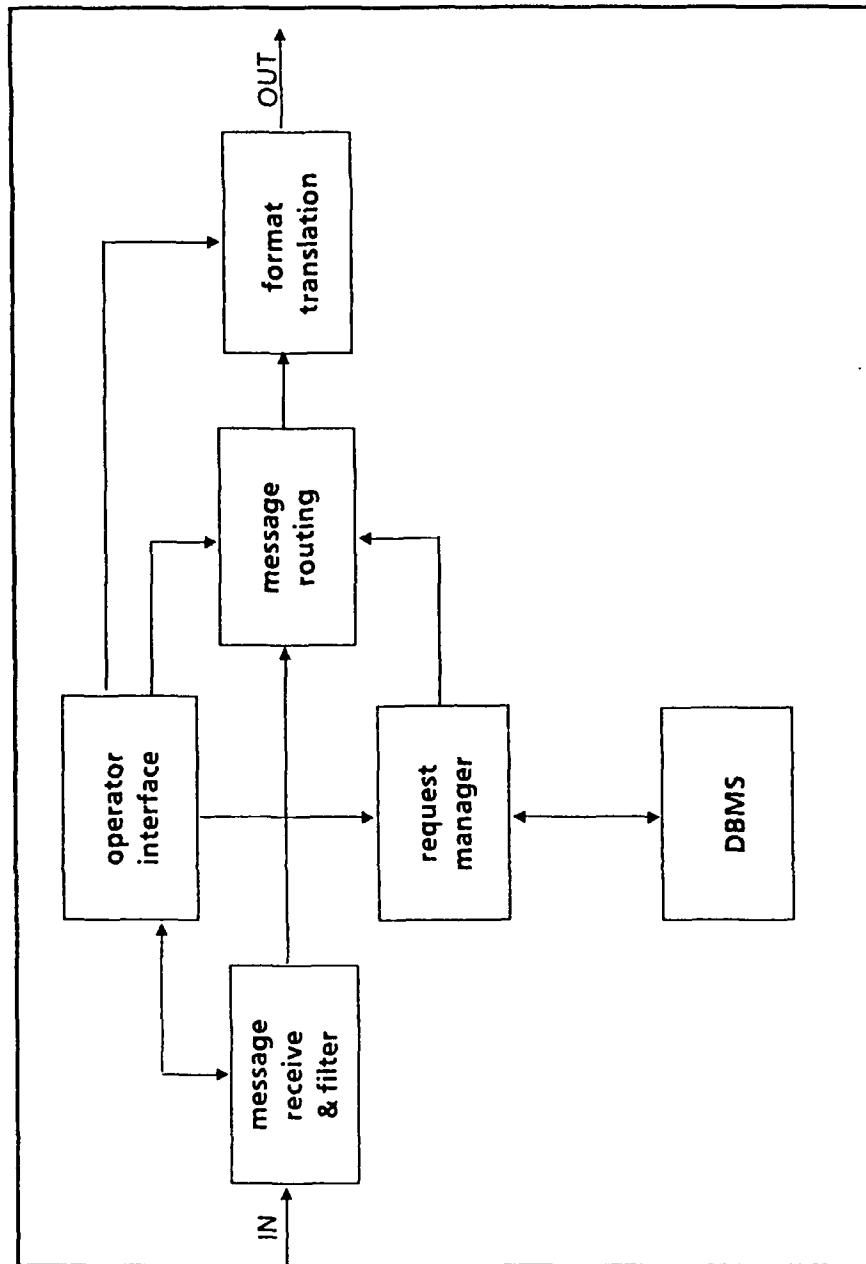
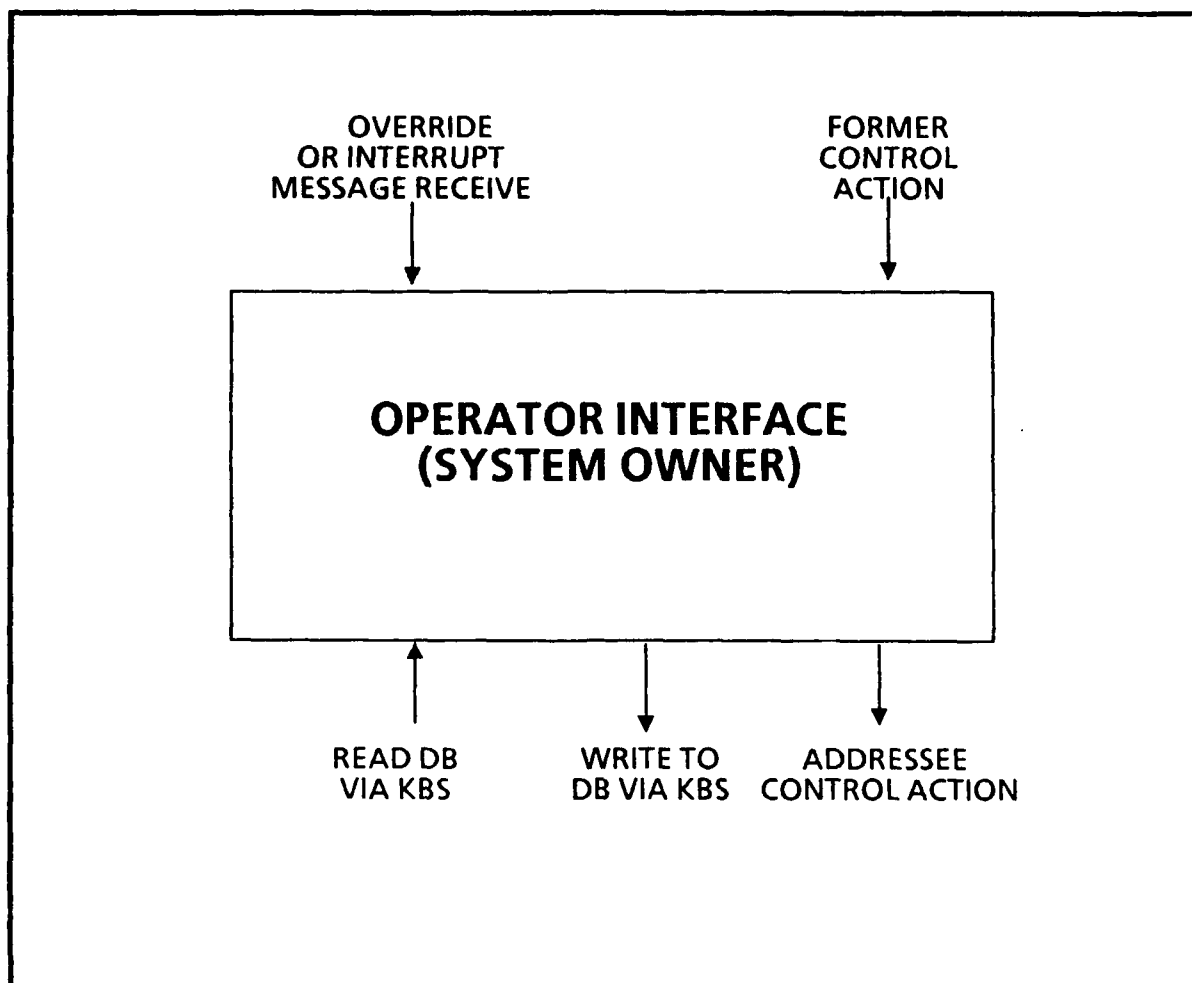Figure 1.   Functional Area Interconnectivity Diagram

41

Figure 2. Flow Analysis for Intelligence Specialist
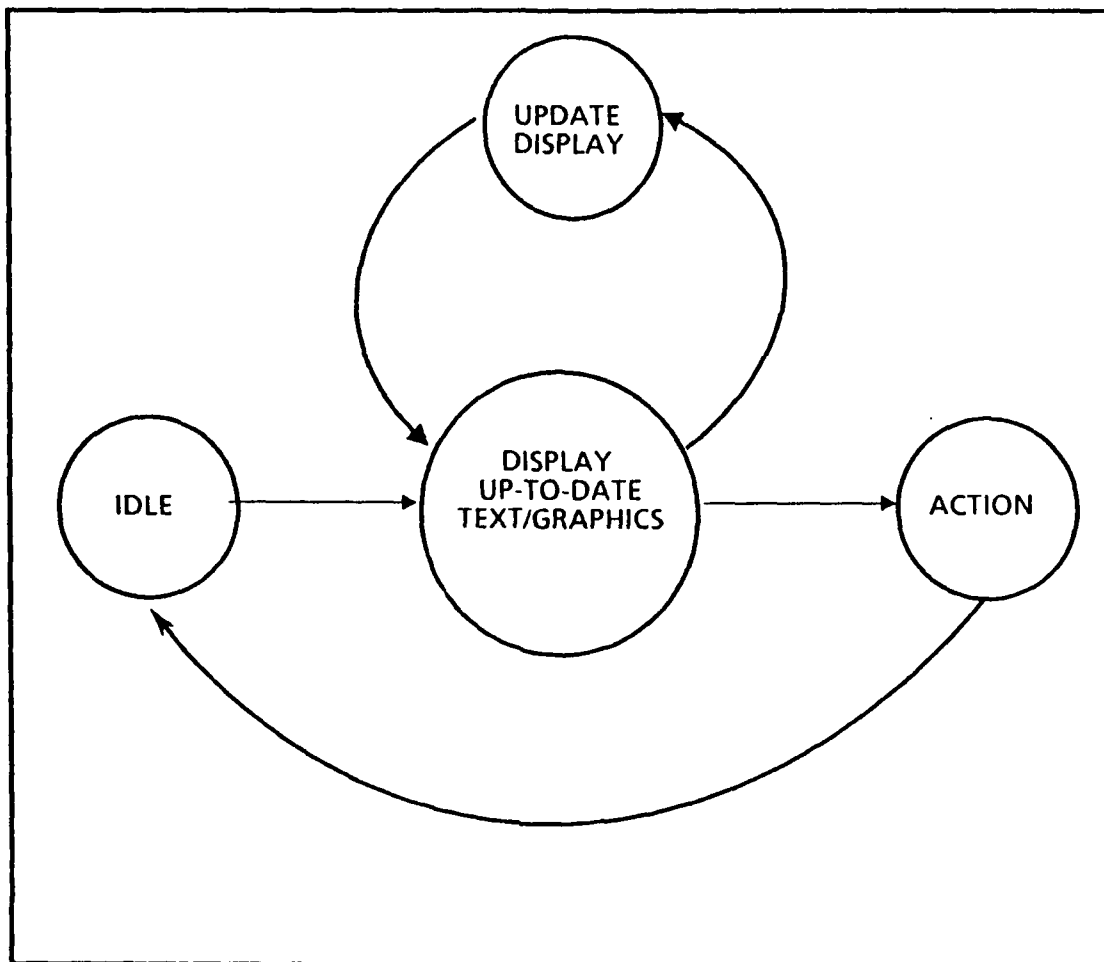   Interface

Figure 3.   State-transition Diagram for Intelligence
             Specialist Interface

43

The text output is displayed in a text window overlay. In this way, multiple pieces of information can be simultaneously displayed. The text will be retrieved from any of the databases: message-log, request-log, request-search, addressee, enemy situation, friendly situation, intelligence-workbook, enemy order or battle, and terrain weather.

Primary output should be a graphic representation of the map overlay. Standard military symbology can be used to maintain an automated enemy situation overlay and the friendly situation overlay. Update and bookkeeping functions would be accomplished by the KBS without operator prompting.

2. Message Receive and Filter

The purpose of the Message Receive and Filter is to provide the means where all incoming messages and requests enter the KBS (see Figure 4). It accepts messages from the operator as well as the system. It then parses the formatted message into message objects, checks information for validity based on each message object and message type, and forwards the message objects to the knowledge base or database and message routing. In the case of a request, the request code is forwarded to the request manager. At any time, information inconsistent with the rule-base or knowledge base, the system

44

notifies the operator through the use of an explanation facility via the interface. The State-transition Diagram (Figure 5) represents the states that the Message Receive and Filter functional area can be in.

3. Request Manager

The Request Manager is responsible for logging all queries for information to the system (see Figure 6). It will pass control to the database manager based on the appropriate request code. If a search is found, it will generate a response with the data from the database. It is the metasystem that is an integral part of this module that actually determines when to pass control to the database manager, and what to do a search is completed. Additionally, the metasystem passes control to the Intelligence Specialist based on the appropriate request code. It then forwards the responses from the DBMS to the Message Routing (Figure 7).

4. DBMS

The DBMS module performs functions within the KBS but outside the realm of metasystem control (Figure 8). Commands for the DBMS are unique and separate from those of the KBS. In this way, the system coordinates functionality between the KBS and the DBMS, but is not fully integrated into one unit.
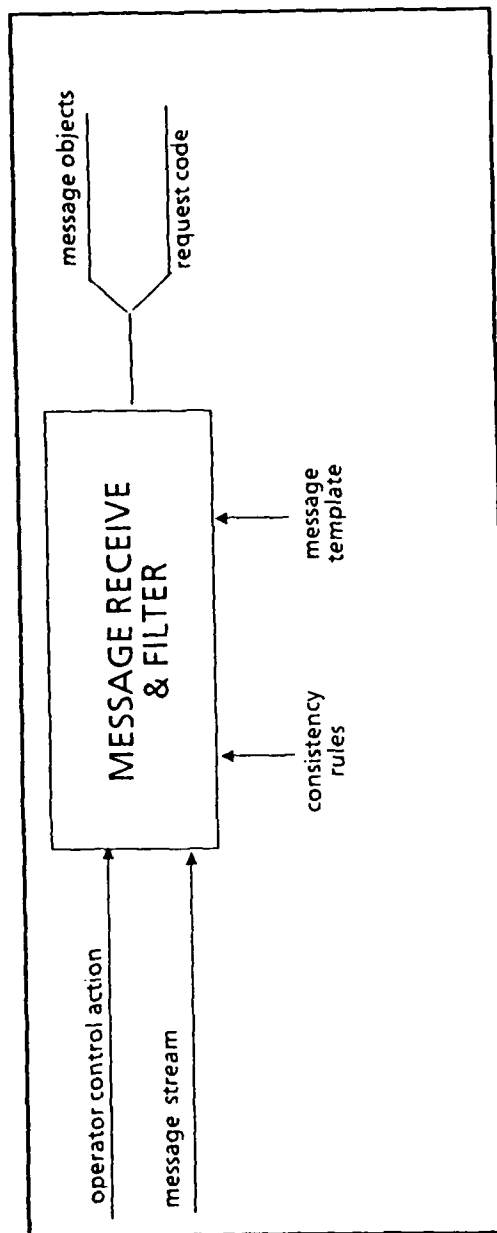
Figure 4. Flow Analysis for Message Receive and Filter
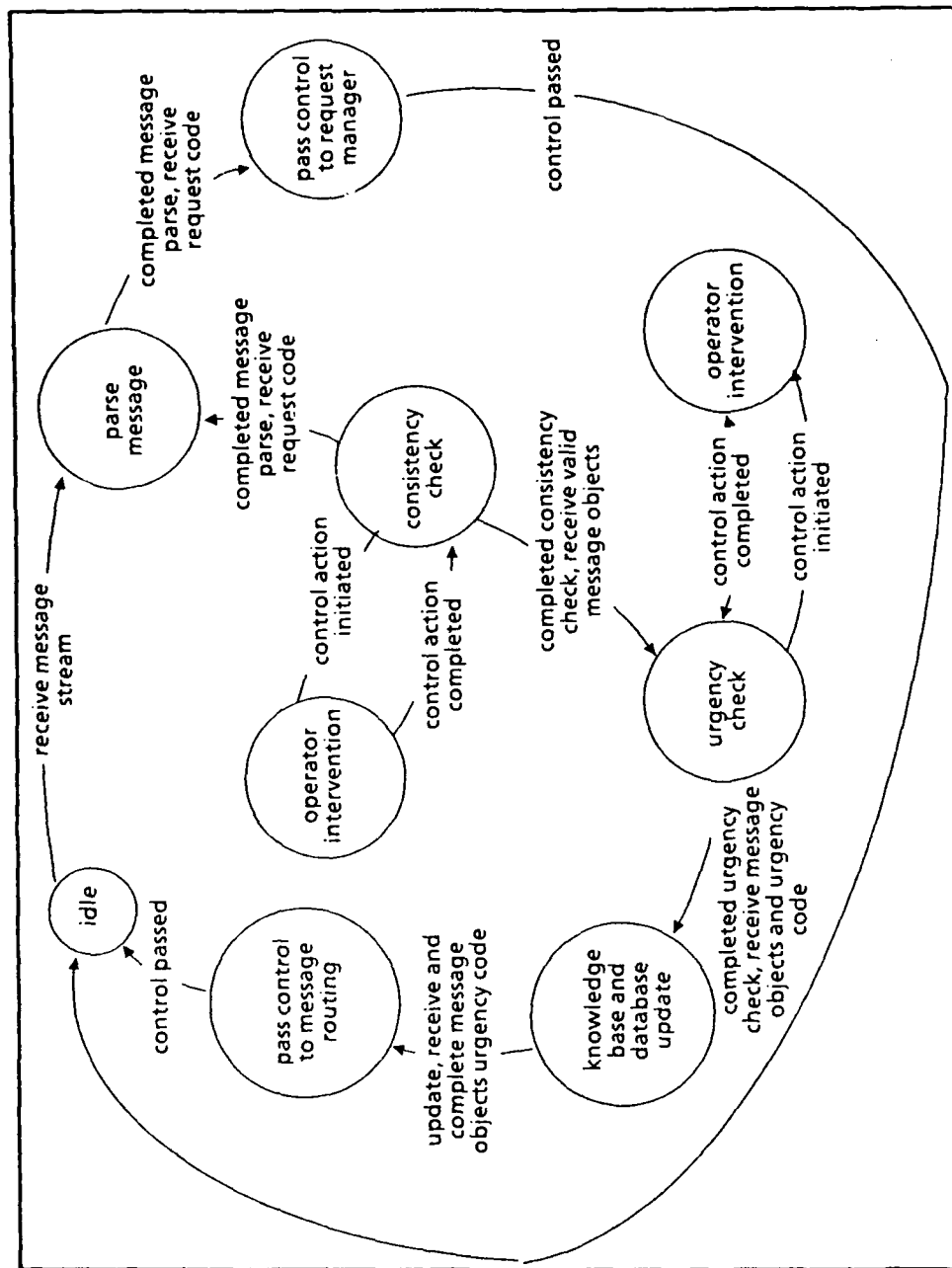
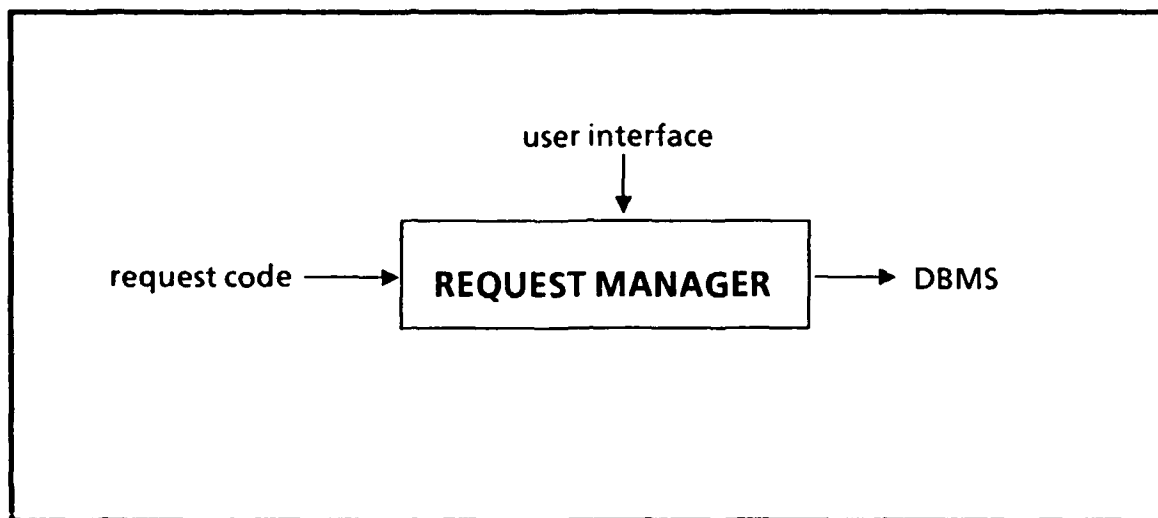Figure 5.   State-transition Diagram for Message Receive
            and Filter

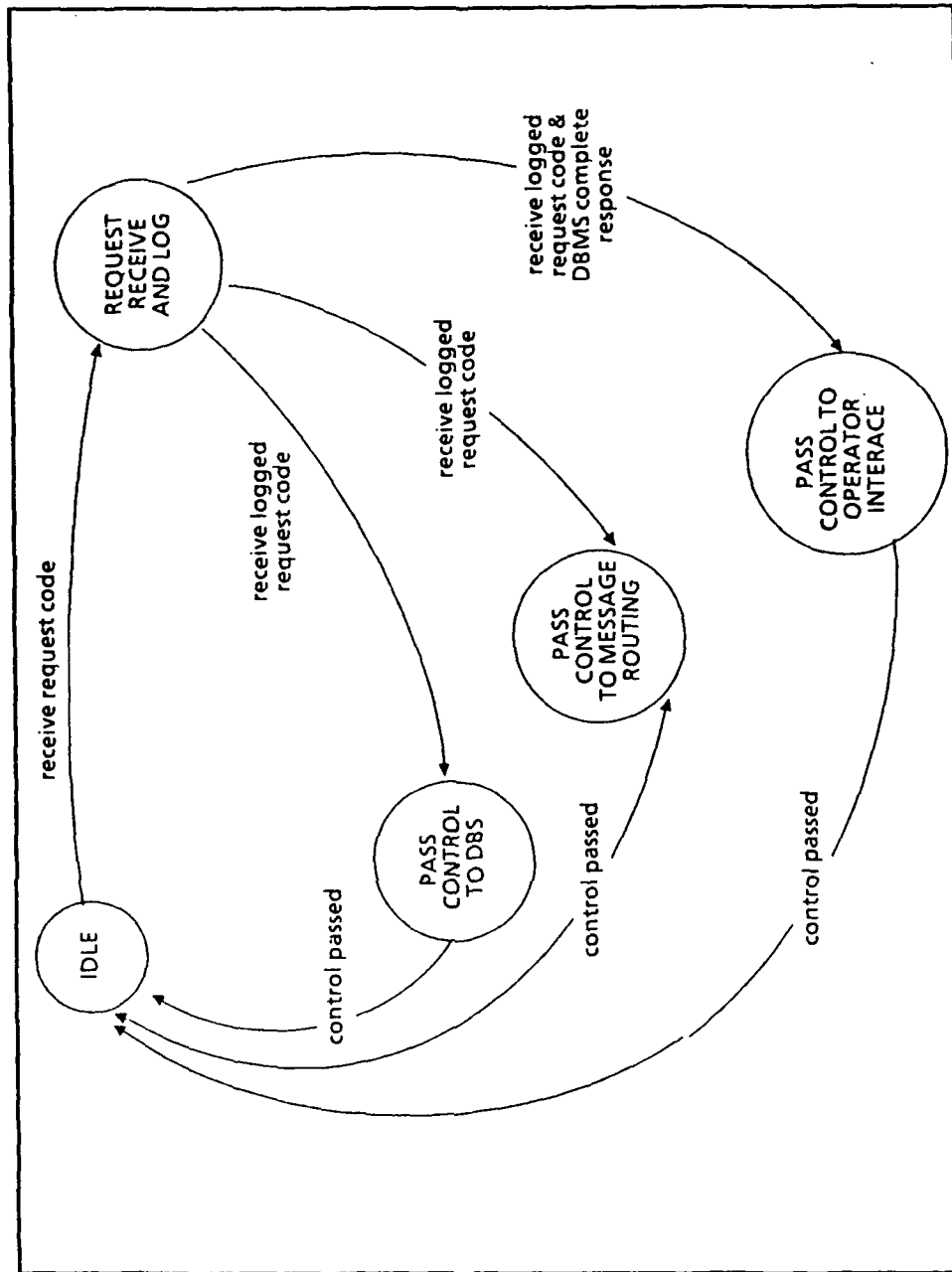47

Figure 6.   Flow Analysis for Request Manager

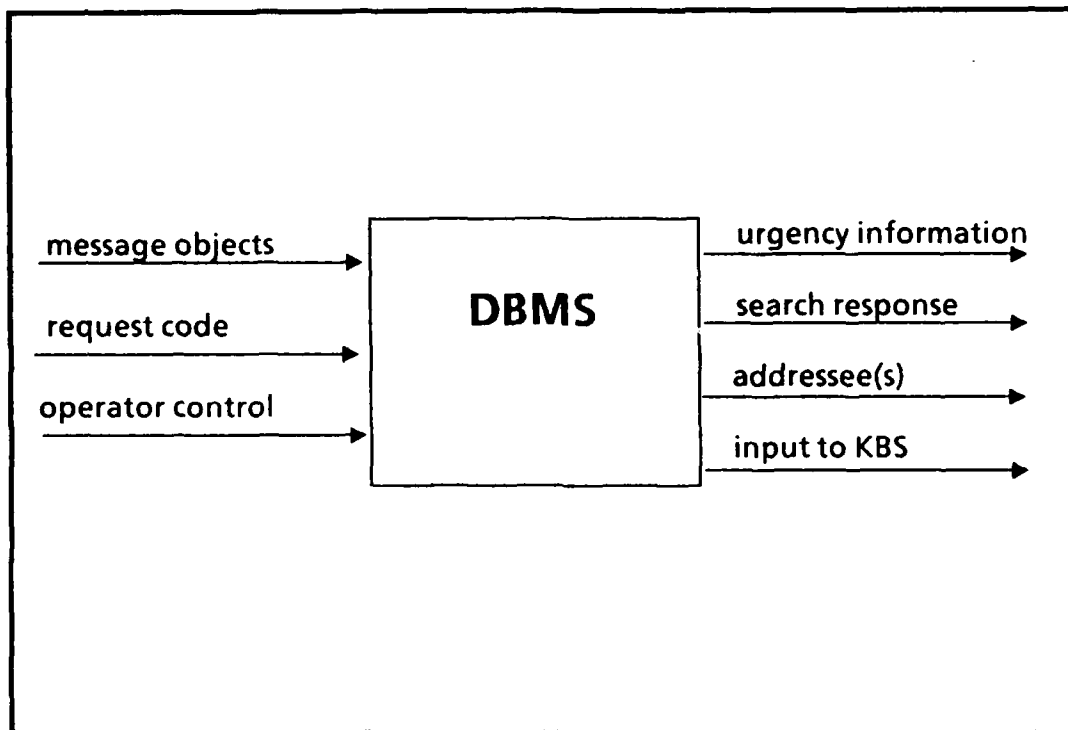Figure 7.   State-transition Diagram for Request Manager

49

Figure 8.   Functional Flow Analysis for DBMS

The DBMS provides information in response to requests from field users as well as from the Intelligence Specialist. It maintains the databases from updates posted to it by the KBS. The DBMS prevents modification to the message-log and request-log; provides an audit of all operator control modifications; provides for read-only privileges to certain data and provides its own databases security scheme. The DBMS State-transition Diagram (Figure 9) illustrates each state given a query to it.

5. Message Routing

The Message Routing KB-module creates a list of addressees, or recipients from the addressee database based on message objects, urgency rules, routing rules, and operator input (Figure 10). It provides for operator control of actual recipients if it is decided that the system-generated list of recipients should be modified. It also matches message objects to addressees based on urgency rules, routing rules, and operator input. Thus, only that intelligence which is needed by each recipient will be passed. The State-transition diagram (Figure 11) for Message Routing illustrates the possible states of the Message Routing KB.

6. Message Format Translator

The Message Format Translator KB places information to be sent in a proper format based on format rules and the

message template database. It produces customized message formats and ensures only pertinent information is reformatted and sent to the appropriate recipients (Figure 12). It calls an external routine or program that transmits the entire message. Each outgoing message is printed out in hardcopy form in case of system failure. Automatic printing of this routine task frees the operator to perform his qualitative tasks. Information which cannot be formatted is presented to the Intelligence Specialist Interface for operator control action. The State-transition Diagram for the Message Format Translator (Figure 13) shows each state of its operation.

C. PROBLEMS, LIMITATIONS, AND CONSTRAINTS

Problems, limitations and constraints in the current system are listed within the categories of problems, opportunities or directives. The following issues were uncovered in interviews with Marine Corps intelligence personnel from the First Marine Division.

- Performance issues, measured by the throughput of the message-processing, based on a fixed error rate that should approach zero percent. Those interviewed contend that retransmission of any message should be avoided. Any messages that have to be retransmitted due to errors places an extra burden on those who are involved in the transmission of the messages. Additionally, due to the short time value of much of the tactical intelligence gained from field units, the information from those messages may no longer be real-time or relevant to those who need it.

- Information issues, where it is either not in a form useful to Intelligence Specialists or Commanders, is not timely, or where irrelevant information is passed.

- Control measures in-place to ensure that intended recipients receive all the information that is pertinent, and that the information is received (or passed) in a timely manner. These control issues include maintenance of the status overlays and other bookkeeping functions currently performed by the intelligence personnel in the COC.

- Personnel effectiveness issues, where effective use of personnel in the COC and in the field units is maximized.

- Service issues, that is, issues from the users perspective concerning accuracy of intelligence received, reliability of receiving that intelligence, and receiving that information in a form that is useful to them.

1. Performance Issues

The time required for sending the radio operator to transmit and receive subsequent acknowledgement of a message is lengthy and often unacceptable for longer or larger messages. The term "unacceptable" is subjective, yet every Intelligence Officer interviewed used this descriptive form. "Unacceptable" also coincides with the author's experiences with transmitting tactical messages.

The amount of messages that the battalion COC can receive and evaluate, and therefore act upon, is very low due to the manual orientation of all tasks. Those interviewed contend that additional personnel are needed to thoroughly evaluate and analyze every message.
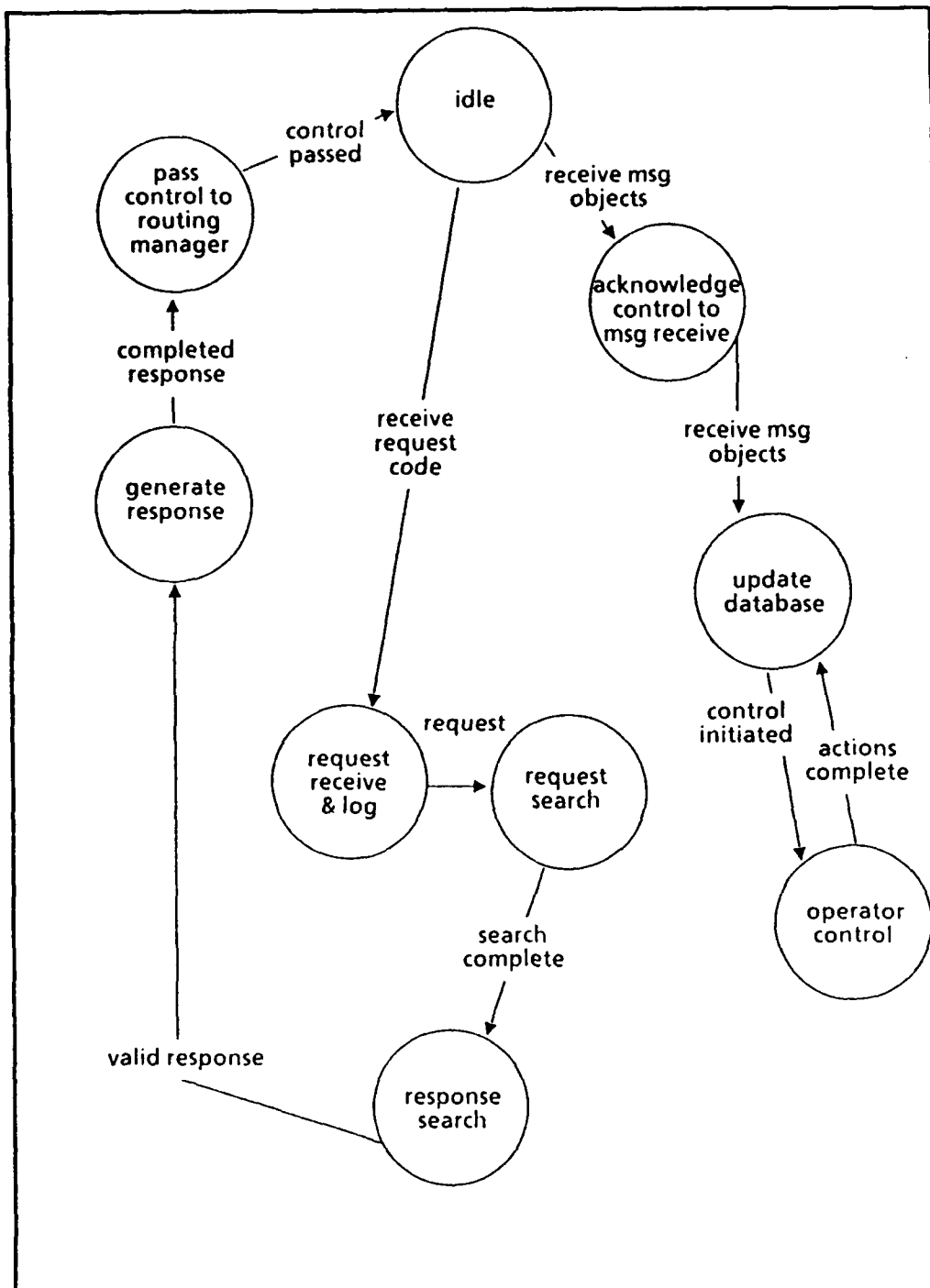
Figure 9.   State-transition Diagram   for DBMS
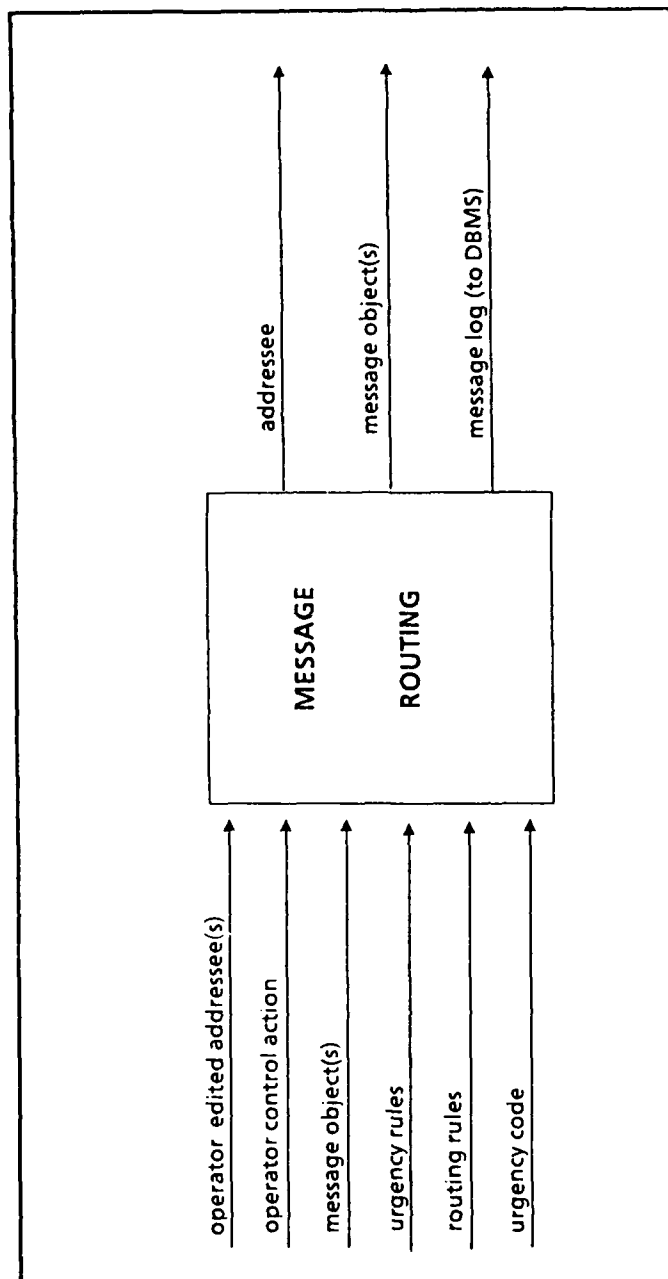   Interconnectivity

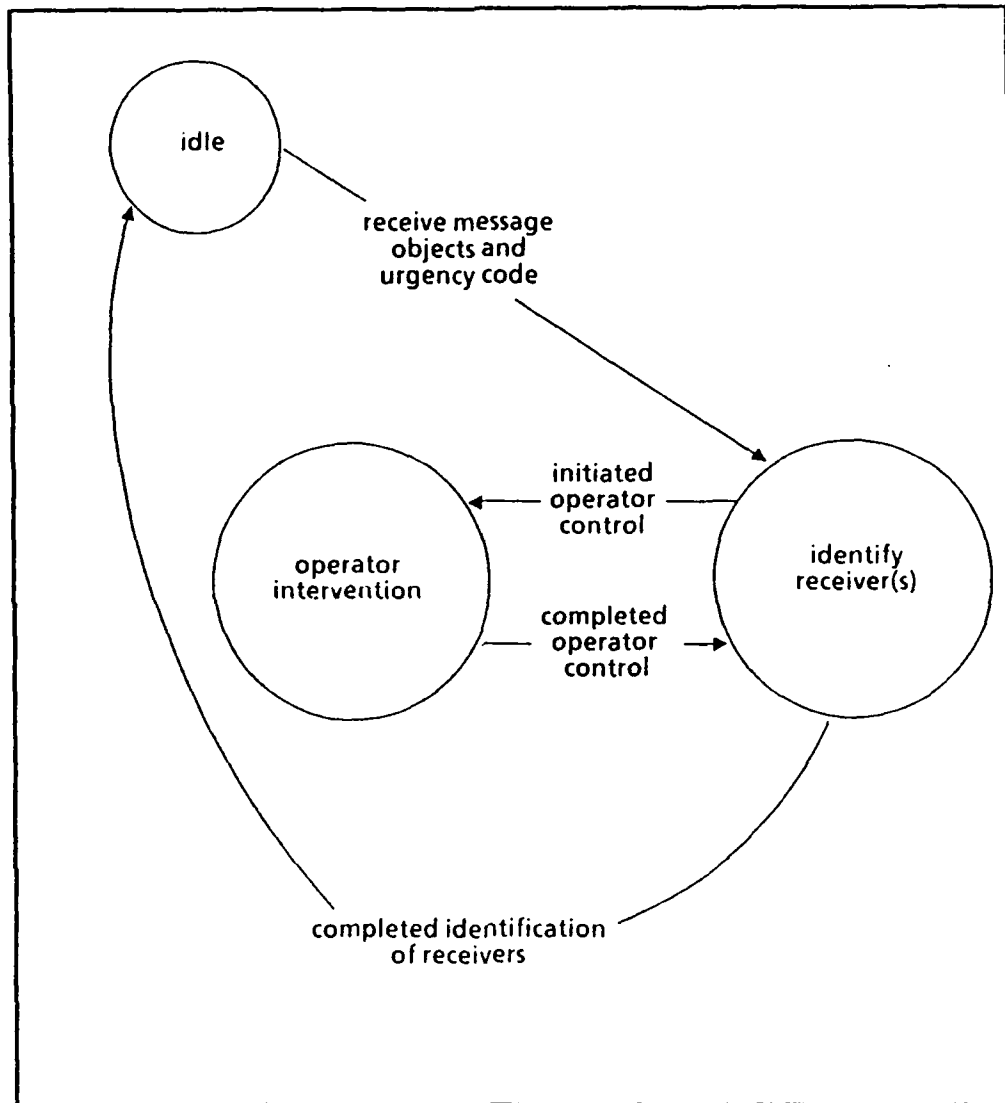Figure 10. Functional Flow Analysis for Message Routing

Figure 11. State Transition Diagram for Message Routing
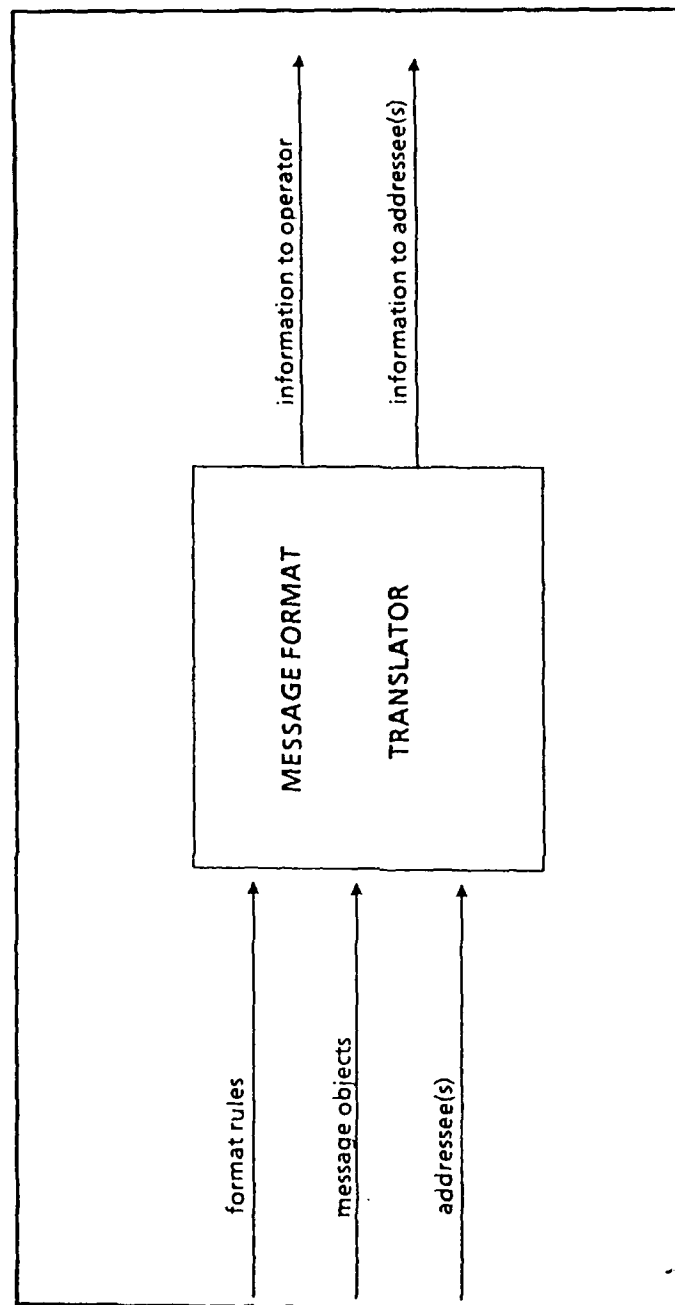
Figure 12. Functional Flow Analysis for Message Format Translator

57
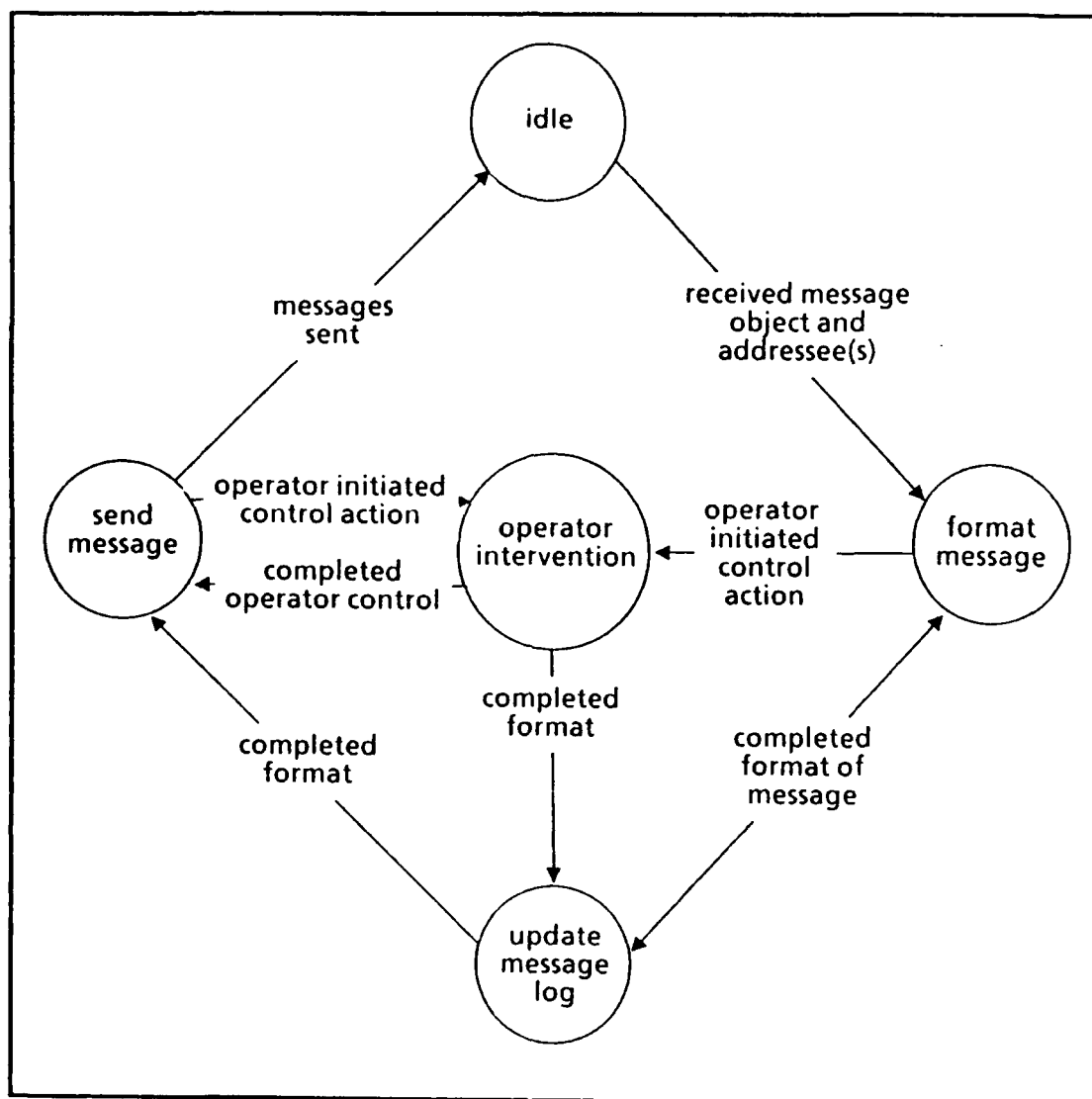
Figure 13. State-transition Diagram for Message Format
Translator

The response time for the battalion COC to respond to routine requests for intelligence is extremely slow. The current standard operating procedure is to send information by messenger in an attempt to keep radio traffic to a minimum. Radio traffic by doctrine is minimized in an effort to prevent the enemy from discovering friendly radio frequencies through signal exploitation methods.

The performance of company and battalion message-authors in drafting messages is degraded by the use of code-words, fatigue, time constraints, and understanding the meaning of message formats. It has been the author's experience, and it has been confirmed through the interviews with intelligence personnel, that the time to draft a message is longer in order to lookup the applicable code-words. The time to evaluate or analyze this same message is longer for the same reason. Additionally, in sending messages during an actual engagement, or while on the move, is difficult because those in the field do not always have time to stop to draft and send a message, and perform other important tactical tasks.

The performance of all hands is degraded by inclement weather due to the manual orientation of pen and paper.

The performance of all hands is degraded by an increased tempo of operations. Human operators can only write and talk at a certain fixed rate in order for others to understand their communication. Going faster and faster to process more information in the same time period causes people to make more mistakes.

The current system does not operate to acceptable standards during COC displacement. Although "acceptable" is a subjective term, all personnel interviewed acknowledged that a significantly lessened amount of information, and in some cases, no information, is processed during COC displacement.

The performance of Intelligence Specialists is constrained by their ability to quickly locate information when hardcopy publications are referenced for information retrieval.

2. Information Issues

The information, as it arrives in the battalion COC in message format, is not always in a form useful to all intended recipients. Most messages contain text which must be plotted on a status board or situation map to be understood. Further, some messages contain code-words and references to previous messages, which must first be referenced.

Irrelevant information is passed in messages. Due to the rigidity of the messages formats and abilities of radio operators, all lines in a given message are included in the text, even though that line may be marked as not applicable. Additionally, not all intended recipients need the entire message every time one is received.

The information is not received in a timely manner. Tactical intelligence is generally useful for only a short period of time, beyond which it no longer retains the same importance. Field units that are unable to transmit a time-critical message may wait too long to try retransmitting it at a later time.

The information passed within the battalion COC is redundant. Four or more copies are required to route to all shops in a timely manner. The shops are the S-2 (Intelligence), S-3 (Operations), FSC (Fire Support Coordinator), Watch Officer, and others as required. No mechanism exists to ensure (before routing) two units do not report the same information, as in the case of BDA (Battle Damage Assessment) reports.

The economy of communication assets is lowered by the present system. Information is passed over several nets, depending on the information and primary use of the net.

There are separate nets for tactical reports and intelligence reports. Present net frequencies were allocated before the advent of computer use in communications. Nowadays, data transmission using computers is measured in fractions of a second.

The information contained in different intelligence databases (journal, workbook, and notecards) is redundant and not in a form readily useful to management. Intelligence Specialists must manually search through their (or someone else's) notes to retrieve information.

3. Control Issues.

The inadequate control of message routing within the COC requires each shop obtain their own individual copy of each message. The Watch Officer may route irrelevant information, or fail to route relevant information to potential recipients. The Watch Officer's intuition, aided by some guidance from the Battalion Commander, is the only control mechanism in place to ensure that those in need of information receive it.

The Watch Officer must initial all incoming and outgoing messages to ensure he has knowledge of their content. This control is placed here at this point in an attempt to ensure that the Watch Officer remains appraised of the

situation as it develops, that all outgoing messages are in correct format, and that information of an urgent nature is properly handled.

Each shop maintains their own logbooks. Logbooks contain essentially the same messages, but exist in an attempt to maintain an audit of actions taken by each shop.

The flow of information contains excessive layers of handling for documentation purposes. Radio operators, not associated with any shop, receive the message and pass copies on to each shop, plus the Watch Officer, who in turn takes action and document their actions taken.

4. Personnel Effectiveness Issues

There is inherent decreased output with the current manual system, which is decreased even further when the tempo of operations escalate, due to the additional information required fora more detailed analysis. In some cases, there is not enough time to give a more detailed explanation even though a more detailed explanation may be appropriate. The intelligence personnel interviewed stated that in order to perform all their required tasks, additional personnel would be needed to perform the bookkeeping tasks.

5. Service Issues

The accuracy and legibility of incoming messages is degraded by the level of experience of the radio operators who send and receive the messages. Communicators who do not understand the message formats or have poor writing skills can negatively impact information processing.

The reliability of evaluation of the information into useful intelligence isdegraded by higher levels of operational tempo. Intelligence Specialists do not always have adequate time to devote greater effort towards analysis, due to bookkeeping distractions.

The reliability of message-traffic routing within the battalion COC degraded by an increased tempo of operations. This accounts for the additional controls in-place in an effort to minimize mistakes. As personnel within the COC get busier, some of their more routine and less critical tasks are not performed as timely as they ordinarily would be, if the operational tempo was not has high.

The coordination between the radio operators, Intelligence Specialists, and Watch Officer is degraded by the level of experience and tempo of operations within the battalion COC. Each agency must complete its own

responsibilities, and in so doing, may not coordinate the needs of the other agencies of the COC.

The coordination between field units and the battalion intelligence section is poor due to the level of effort required for information retrieval and communication, and lack of a clear understanding of what to ask for. Field units generally have a need for information in a time-critical manner, and do not desire, or simply cannot send a messenger to the COC to obtain additional intelligence.

The flexibility of the radio operators to accurately record or send message in nonstandard format is dependent upon the experience level of the radio operator and intended recipient. The radio operators are in effect only copying messages onto paper for others to read. Code-words, technical words and other keywords may not be understood by those who have no need to know the content of the messages. The messages that are recorded are sometimes difficult to read by others, or are copied wrong by the radio operators. Each recipient must then decode the message.

The reliability of intelligence is degraded by the lack of detailed, up-to-date intelligence maintained for reference by the intelligence section. Updating intelligence on a regular basis and under all circumstances is difficult

for the Intelligence Specialist to consistently perform, for there are other duties which are of higher priority that also must be performed.

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

It is difficult to draw concrete conclusions concerning the applicability of a knowledge-based system to integrate the collecting, processing, and dissemination functions of tactical intelligence in a real-time mode. However, there is a high probability that such a project is technically feasible; and that collecting, processing and disseminating information can be captured in knowledge-bases. All routine tasks should be automated, freeing the Intelligence Specialists and Officers to perform their intuitive tasks and qualitative decision-making. Additionally, automating message handling and bookkeeping can eliminate the need for extra radio operators in the Battalion COC. In doing so, however, one must weigh the costs in terms of reliability of the knowledge-bases, speed and dependence on automation, against the virtues of humans performing the same tasks. Using these factors for comparison, the option at this point tends toward automation: structured redundant tasks would be performed in a more consistent manner. Information distortion is likely with multiple layers of manual processing involved. However,

no claim can be made concerning the optimality of search of representation of the knowledge-base at this early stage.

The commercially available expert system NEXPERT was chosen for its fit to the adaptive design approach: it lends itself extremely well to prototyping. A discussion of its architectural limitations with respect to its adaptability for field use should be a topic for further research. It does appear feasible at this point to use NEXPERT as the expert system of choice for a personal computer-based artificial intelligence application for technical intelligence. Particularly interesting were the editors that allowed ease of knowledge entry and subsequent modification, and the semantic networks that presented pictorial flows of objects and rules. In effect, the domain-expert that is, the Intelligence Specialists, may be able to be the Knowledge Engineers, subject to their qualification as an "expert" of NEXPERT.

Several issues arose when considering an expert system for use in a tactical environment:

First, can an expert system be adapted to a combat environment and remain reliable? The system must possess significant knowledge capabilities to handle the large variety of scenarios that will occur in the field. In constructing

the system for this eventuality, general rules must be constructed and the inference engine then can reason from these "top-level" facts. Allowing the system to reason on general rules or approximations means that goals need not be meticulously exact (Zytkow and Erickson, 1987, p. 141). If new facts or new conclusions are drawn, the inference engine must incorporate these newfound conclusions and facts into the knowledge-base, and they must be correct.

Is it possible to maintain the system to meet the users' demands? It is expected that as any tactical scenario develops, different constraints will be in place at different times. Essentially, the rules may change as the game is played. Further research is required for the dynamic control of these changing rules. If the rules are changing, then the procedures which maintain their correctness and validity are major research issues (RADC, 1986, p. 4-19). The system should be constructed entirely of user defined choices, constraints, and satisfiers that can be changed during the life of the KBS. NEXPERT supports this end-user computing through extensive use of its different editors.

This thesis effort has focused upon meta-knowledge acquisition, organized into separate and independent modules based on function, that can be loaded as required to control

the system. Within this context of knowledge representation, there were several assumptions: (1) rule-based formulation could be used to capture the concepts and processes of "rules about rules", (2) an object-oriented KBS accurately captures the structure of the concepts of meta-knowledge, (3) the control structure of the KBS reflects what the experts' problem-solving strategies may be, (4) rules reflect associations and methods that are either used by the experts when solving the problem, or are understandable rationalizations of such methods . These assumptions led to several points:

First, meta-knowledge should be represented by separated global and local elements, and time and event-driven elements. The state of any of the functional areas of the system then, is represented by the combination of object values. The organization of the database and knowledge-base will be considerably different in order to account for the differences of the global and local objects, and time dependent and independent objects. A type of organization recommended for dealing with this problem of a large number of constraints is the concept of frames. Frames representing components or objects of meta-knowledge allow for competing choices (or hypotheses) to be looked at in a top-down fashion, eliminating

possibilities as a result of constraint violation. The higher-level classes and then subclasses are search first, then objects and subobjects are subsequently searched for constraints that cannot be satisfied. Additionally, "The portions of the knowledge-bases that are dynamic must be maintained in a different manner than those portions that are static." (RADC, 1986, p. 4-19)

There were three potential disadvantages that this type of expert system might have:

- First, training the users to become proficient in NEXPERT (but the same conclusion would likely hold true for any robust expert system) would be difficult. Although a recognized software engineering principle seems to support than an expert system should be easy to learn and easy to use, in this case a system robustness should not be sacrificed for system ease-of-use. However, it is too early to make a sweeping conclusion to support the use of an unmodified NEXPERT. Any such modification, though, must be weighed in terms of memory and response time lost against that of maintaining proficiency of the users. A substantial front-end investment may be required to ensure higher system performance and productivity.

- Second, the degree of confidence that the intelligence community places in the knowledge-base and the depth of the knowledge-base was a concern. The size of the potential domain in order for the system to be truly robust might be inhibitably large for a personal computer to handle. It is felt that the modularization and independent organization of the rulebases alleviates this to some degree. Still, some doubt exists as to whether any system can handle any scenario that may occur (even those scenarios not identified in advance).

  However, since this system is based on independent rulebases and modularization, it lends itself to remedying the smaller, easier problems, one-by-one, that in aggregrate constitute the whole problem of tactical

71

intelligence flow. Prototyping each task incrementally and then combining each smaller remedy solves the larger problem. The system, therefore, does not have to provide the whole solution before implementation. Solving each of the component problems, i.e., that of maintaing logbooks, and keeping the enemy situation updated, in turn provides the solution of using the expert system for intelligence personnel in a tactical environment. In the end though, users must be confidently convinced that the system provides an advantage over the other alternatives. (Fick, 1980, p. 139)

- Third, to the extent that building any expert system is still experimental (Hayes-Roth et al., 1983, p. 154), it is too early to predict any success in operational terms, of such a proposed system for two reasons: knowledge acquisition and knowledge revision.

Knowledge acquisition and revision are of primary concern in future development of this system. Given that the inference engine should be transparent to the user, the domain expert, nonetheless, must still be able to change the rules during operational use. Formalization of knowledge acquisition for a system of this scope requires further development coupled with extensive user involvement. Using NEXPERT with its rule-editor, object-editor, and metaslot-editor, knowledge can be quickly and easily organized to promote prototyping. The advantages of such knowledge-base (KB) editors are: (1) They facilitate the task of entering knowledge into the system, (2) they automate bookkeeping functions and allow the knowledge engineer to concentrate on his qualitative tasks, (3) they help the user to avoid

72

typographic and syntactic errors and, (4) they check for semantic inconsistencies (Hayes-Roth et al., 1983, p. 149). These advantages can be realized in a field environment whereby the domain expert (Intelligence Specialist) essentially becomes the knowledge engineer. The use of the KB-editors is another area for further effort.

B. RECOMMENDATIONS

Building the prototype appears to be the next step in creating the system for tactical use. Prototyping in NEXPERT, however, will require extensive efforts in the areas of knowledge acquisition, use of NEXPERT itself, and interface with the chosen external programs and routines.

In attempting to build a version-0 prototype, organizing the classes, objects and rules into components or frames offers an approach that works with NEXPERT. NEXPERT itself, is frame-based and object-oriented. A frame is a collection of facts; the abstraction of an object or set(s) of objects (Rowe, 1986, p. 286). NEXPERT will perform all the bookkeeping functions and by incrementally compiling every new object and rule, provides for error-checking. Each object will get a separate frame with slots in the frame to represent its properties (and properties receive values), and for the whole whose values are pointers to that frame or object.

There are several advantages to frame representation of objects: (1) Frames distinguish properties of components not shared by the whole class, (2) frames describe relationships of the objects to one another, like the relative location of parts of a physical object or the relative time of subevents of an action, (3) frames distinguish multiple of optional occurrences of an object, whose variation is described by qualifying properties and, (4) frames can be generated for different levels of objects: frames for objects describe subobjects in property-slots, and-so-on (Rowe, 1986, p. 286). The slots can also be procedural that represent instructions or sets of instructions to be carried out. Filled slots represent facts, or properties. These slots can then be the object of another frame. For the user who may be called upon to create and delete objects and manipulate slots within the frames during an operational exercise, there may be an advantage of frame representation in organizing and displaying new information. NEXPERT's KB-editors provide an easy interface to modify the KBS as necessary. This feature is particularly helpful during initial loading of the knowledge-bases, since it is predicted that an extensive amount of rules

and objects are needed.   The recommendation, then, is to proceed with development of the expert system through prototype.

APPENDIX

SECURITY

A. INTRODUCTION

Central to a military information system that is expected
to operate under conditions where data integrity is crucial
to success, and where vulnerability reduces that success
potential dramatically, is computer security. Four central
themes establish the baseline for the discussion of computer
security for the intelligence integrated information system:

First, the system is designed to operation in a hostile
environment. The objective is total database security based
on the assumption that the enemy will definitely devote
considerable effort to interception and disruption. The enemy
must be denied access to the databases at all times.
Therefore, proposing countermeasures to decrease the
probability of threat is inappropriate alone. Several
security countermeasures integrated together and used
rultipliciously should be independently evaluated.
Individually, countermeasures decrease probabilities of
threat; collectively, they must deny.

Second, the major security concern is protecting information from leaking to the enemy. Protection from unauthorized use from internal sources during combat should not be a significant factor in the design of an appropriate security scheme. Further, multilevel security may be breached in a life-threatening situation. For example, the author contends if the value of the information will save lives, then the level of security for that information should be disregarded and the information disseminated to those whose lives depend on knowing that information.

Third, it is doctrinally appropriate for threat analysis and identification of countermeasures to be the responsibility of the CounterIntelligence Officer of Intelligence Officer performing counterintelligence functions.

Fourth, there are six fundamental requirements to provide for controlled access to information and assurances that must be accomplished in a trusted computer system: (1) There must be an explicitly and well-defined security policy enforced by the system. (2) Access control labels must be associated with all objects. It must be possible to mark every object with a label that reliably identifies the object's classification level of the modes of access granted to subjects who may potentially access the object. (3)

Individual subjects must be identified. (4) Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible part. (5) The computer system must contain mechanisms, both hardware and software, that can be evaluated independently to assure that the system enforces requirements through the other requirements. (6) The trusted mechanisms that enforce the basic requirements must always be protected from tampering.

B. PROTECTION SCHEME

Proceeding on the premise that security should be designed into the system and not added on as an afterthought, a tactical information system designed for use at battalion level needs a discussion of the security dimension before any system model is considered complete. Unique issues confront such a military system that is designed to always operate in a hostile environment.

It is recognized that system security requirements must meet with the Department of Defense Standard System Evaluation Criteria. A class C2, Controlled Access Protection is appropriate for this type of system. This class of protection scheme is intended for those dedicated mode systems operating in a closed environment. It offers the minimum accepted standards that a class C2 must possess:

78

- Discretionary access control. This mechanism provides that objects be protected from unauthorized access.

- Object reuse. No information produced by one user is available to another user that obtains access to that object.

- Identification and authentication. Users must identify themselves before beginning any actions the trusted computer base (TCB) is expected to control. Authentication data will be protected so that it cannot be accessed by unauthorized users.

- Audit. The TCB will create and maintain an audit trail of accessed to objects it protects. This audit trail will be protected from modification, unauthorized access and destruction. (DOD 5200.28-STD, 1985, pp. 15-18)

C. SECURITY CATEGORIES

In attaining that level of protection of security required, security in the following categories are discussed: operating environment, physical security, communication security, data security.

1. Operating Environment Security

Physical security measures and operational procedures can be emplaced to significantly limit any access (Hsiao, Kerr and Madnick, 1979, p. 47) to the system. The first step, however, is to define the set of authorized users and the operating environment. The operating environment has already been defined as the battlefield. The set of authorized users are: those officers and men who have a need-to-know to either (1) send tactical messages, (2) receive tactical messages and

(3) receive tactical intelligence on the status of either the enemy or friendly situation. Authority to grant user privileges should rest with the owner of the database, and a hierarchal scheme defined. Normally, the battalion commander owns the database. The user list includes company commanders and their radio operators, unit commanders, platoon commanders, company executive officers, and others specifically designated by their respective commanders. Those within the command post include the Battalion Commander, Battalion Executive Offier, Operations Officer, Watch Officers, Intelligence Officer, and the Intelligence Specialists. The user group just defined is extremely small, therefore, it would be appropriate to implement this system as a closed environment. A closed environment, with its few authorized users, provides a high degree of physical security (Hsiao et al., 1979, p. 48). A limitation of this implementation concerns the impact of the availability of the system if the authorized users become casualties in combat, and the opportunity for training for those not designated prior to the outset of system operation.

2. Physical Security

The threat to the physical security of the computer system operation is natural disaster. It does not include

80

theft or tampering. Natural disaster in the context of military considerations needs further clarification. It is considered to include the elements of nature, such as rain and temperature, that impact on the computer hardware operation; and the power source required for maintaining system operations. The countermeasures available to protect the computer system from natural disaster include a reliable computer and encasement, and a continuous power supply.

Computers chosen for tactical use must be capable of operation in any climate and weather. Additionally, it should be expected that rough handling would be the treatment norm. The feasibility of fielding such equipment is proven with similar systems already in place.

Power supply is also considered a countermeasure. Disruption of the power source would significantly affect the operation of any computer. For the Marine Corps, normal electrical power is supplied to the command post by a diesel generator located a short distance away and connected via cable. The author opines this source is unacceptable as a power source for computers. For tactical considerations, its signature is audible for quite a distance. It is highly unreliable, with frequent power surges and outages. An alternative is battery power. Use of batteries ensures the

portability of the computer for routine COC displacement and in case of a hasty relocation. Also, the computer would not be dependent on the reliability of the diesel generator. "As the reliability of computers has pushed above the 99 percent mark, the most common cause of equipment outage has become power failure." (Carroll, 1987, p. 117)

However, these countermeasures contain limitations. In any military system that requires a power source for operation, the transport of that power supply is a logistic nuisance. A unique battery-pack or generator, used only for the computers, should not be used for that very reason. Instead, the standard batteries used with current FM radios should be used. Each battery can deliver up to six hours of continuous operation (with the radios). Configuring computers to accept that as the power source would be a plus for those who have to man-carry such gear.

Authentication and Identification threats also exist under the category of Physical Security. Appropriate countermeasures to overcome this threat are passwords, keys, and handshaking. A combination of passwords and handshaking should be used. It is probably this intrusion point that is the most vulnerable to attack, and most likely to be attacked. Interception of communications is a favorite enemy collection

method (FMFM 2-1, 1980, p. 101), and the enemy must first penetrate the system in order to access data or intercept messages. Since callsigns that are already in use are classified information, and their distribution limited, their use as passwords can be considered. For example, Company A's callsign for a period of time may be R2B; therefore, Company A's password would also be R2B. However, passwords alone are not enough (Chalmers, 1986, p. 73).

Further discussion must include mechanisms to detect instances when an intruder is attempting to access the system. An interrupt or flag can alert the system security officers if a predetermined threshold of entry attempts is exceeded. Handshaking is considered a counter-countermeasure. In the event of entry into the system via the correct password, but under suspected methods or circumstances, the user must provide a series of passwords or pass-statements to an algorithm even though the user doesn't know the algorithm (Hsiao et al., 1979, p. 98). The algorithms, like passwords, must be changed at frequent intervals and be protected. Also, individual algorithms for each different user should be considered.

There are limitations to using keys and having passwords. Keys, although normally considered a

countermeasure contributor in most literature, should not be used in a combat environment, if it is a key that is carried. Its loss not only compromises the key, but implies that the authorized user could not gain access. This occurrence could happen when the user most needs urgent communication. Passwords can be compromised by loss or unauthorized distribution. Additionally, they must be changed frequently.

3. Communication Security

The threat to communication security is transmission security, that is, ensuring that all transmission remain secure. Countermeasures to oppose this threat include cryptographic transformation and meditation certification.

Cryptographic transformations are techniques for encoding data to hide their content in the course of communications in the network (Hsiao et al., 1979, p. 135). Cryptographic techniques for secure telecommunications can be applied throughout the network, including line encryption. Since all data transmitted through an otherwise unsecured net is encrypted, it is considered secure (Gilhooley, 1980, pp. 33-56). To penetrate an encrypted transmission, an enemy must have a high work factor value. The work factor depends on the amount of encrypted text available and the time it takes to break the cipher (Carroll, 1987, p. 175). The value is

reduced by cryptographic systems in which the key is readily apparent; systems that infrequently change keys; availability of cryptographic devices, program and keying data to the enemy; malfunction of cryptographic equipment; and poor security practices on the part of the users (Carroll, 1987, p. 182).

The mode of operation for the terminals should be the transaction mode (Carroll, 1987, p.167). In this mode, the user is constrained to work only within the confines of the specific application program. In order to do this, the program should have two main characteristics: mediation and certification.

Every input should be mediated in such a way that it is checked for validity before being passed to the central computer. This is called mediation. For such a tactical system, validation may include checking for anticipated input errors, consistency in message information and data requests, and parity checks. Mediation means that only permissible, certified commands will be allowed to enter the computer (Carroll, 1987, p. 167).

Every permissible command and every permissible sequence of commands should have a predictable and acceptable response. This is referred to as certification. No

modification of the applications program or operating system, or database should result. (Carroll, 1987, p. 168) For example, a mechanism emplaced may allow only an APPEND data to be acceptable.

The limitation of mediation and certification may include limiting the set of allowable commands. However, in doing this, the power of the DBMS may be severely limited.

Cryptographic transformation offers a flexible and secure means of data security. If the use of keys are used to determine the ciphers, and these keys must be carried, it is anticipated that the keys can be compromised by loss.

4. Data Security

The threat to data security is passing value-sensitive information to unauthorized recipients. Countermeasures that lessen this threat are view mechanisms and query modification.

Access decisions to a tactical database should be based on value-sensitive information and state-sensitive information. Value-sensitive information is context-independent and is based on the current value of the data (Hsiao et al., 1979, p. 224). For example, to prevent "information overload" (which can be viewed as an independent consideration in addition to security) to a Battalion Commander, a value-sensitizing information mechanism would

ensure that users could only view pertinent information specific to that battalion, and other criteria established in the design of the database.

State-sensitive information is also context-independent information in which the dynamic state of the database management system plays a role (Hsiao et al., 1979, p. 224). If a suspected intruder is attempting to access a file (perhaps identified through the handshaking mechanism), the Intelligence Officer, as owner of the systems, places it in a locked state to prevent files from being accessed.

View mechanisms makes the user see only what they need to know. Attribute information called schemas are provided access control by subschemas. Different subschemas may be assigned for different users (Hsiao et al., 1979, p. 226).

Query modification disallows user access to information by modifying any query that attempts to gain access (Hsiao et al., 1979, p. 227) to information that a user is not authorized to view. Again, the user only gets to see data on a need-to-know basis.

An added benefit of these security countermeasures is that the unit commander views only what would be pertinent. Extraneous data from the database would be filtered and would be prevented from being viewed. Remember, the user may be in

actual combat and may not have time to browse through data. Both view mechanisms and query modification not only protect the commander from unnecessary information retrieval, but more importantly, limit the amount of compromise sustained.

Allowing only certain information to be viewed or accessed by a user may prevent that user from obtaining that one piece of data that is needed. Additionally, all commanders want to personally pick and choose which information is or is not needed; it is not likely that commanders rely on a computer to make sure important decisions of that type.

Another threat to data security is the accessibility of the actual data. Countermeasures to restrict data access include partitioning, compartmentalization, the security atom concept, and improving access precision.

Once an access decision is made by the DBMS, requested data will actually be accessed. A goal of the system is that of absolute precision, which means every piece of data accessed is a piece of data requested (Hsiao et al., 1979, p. 233). However, the "pass-through problem occurs when the DBMS, in order to get certain data, must access some other data which have different protection requirements." (Hsiao et al., 1979, p. 235) If the database is partitioned into

groups, and if the DBMS knows the security property of each group, then the system will go access the records of those groups directly whose security properties do not deny the request (Hsiao et al., 1979, p. 236).

The security atom concept compartmentalizes the database into partitions. By assigning different protection attributes to different security atoms, the records of an atom are protected uniformly (Hsiao et al., 1979, p. 236). Such a concept is appropriate for tactical use for two reasons: (1) denial of information from the enemy,and, (2) prevention of other friendly forces from gaining access to information which does not contribute to the mission accomplishment. Here the security atom usage is quite unique. The expected protection concept implies that a proper clearance would be required in order to view the atom. For tactical use, where the level of security is not the mechanism that determines access, the security atom protects the information nonetheless on a need-to-know criteria.

5. Conclusion

Designing security into a system model for further development must be exhaustive. Security of information should be a primary focus of a tactical database. The considerations for employment of security concepts, with their

possible limitations have been presented as independent modules to incorporate into the design of the DBMS functional area of the KBS. No greater emphasis is placed on one area than another, for concentrating efforts in one area leaves gaping holes elsewhere (Gilhooley, 1980, p. 35). Independent modularity of countermeasure implementation ensures a layered security protection scheme that only a sophisticated, dedicated, and resource-rich enemy is likely to penetrate and exploit. This author opines that immediate tactical information is of lesser importance than strategic intelligence. tactical information tends to be useful for only a short period of time. This short time value of data concept allows for a less vigorous protection scheme. The security issue should focus on the length of time that the data must be denied to the enemy. Before a tactical database is built, the concepts of computer security must be mapped into the specific implementation scheme, and will form the basis for doctrine when the system is operational.

LIST OF REFERENCES

Begeman, Michael L., and Conklin, Jeff, "The Right Tool for the Job," *Byte*, pp. 256-267, October 1988.

Carroll, D., *Computer Security*, 2d ed, Butterworth, 1987.

Chalmers, L.S., "An Analysis of the Difference Between the Computer Security Practices in the Military and Private Sectors," *IEEE Symposium on Security and Privacy*, 1986.

Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, 1985.

Fick, Goran and Sprague, Ralph H. Jr., *Decision Support Systems: Issues and Challenges*, Pergamon Press,1980.

Fiderio, Janet, "A Grand Vision, *Byte*, pp. 237-246, October 1988.

Gilhooley, I.A., "Data Security," *Advances in Computer Security Management*, v. I, Heyden and Son, 1980.

Hayes-Roth, Frederick, Waterman, Donald A, and Lenat, Douglas B., *Building Expert Systems*, Addison-Wesley, 1983.

Hsiao, David K., Kerr, Douglas S., and Madnick, Stuart E., *Computer Security*, Academic Press, 1979.

Korth, Henry F., and Silberschatz, Abraham, *Database System Concepts*, McGraw-Hill, 1986.

Nunamaker, Jay, F., Jr., et al, "Crisis Planning Systems: Tools for Intelligent Action," *Proceedings of the 21st Hawaii International Conference on System Sciences*, Computer Science Press, 1988.

Rowe, Neil C., *Artificial Intelligence Through Prologue*, Prentice-Hall, 1986.

Rome Air Development Center (RADC), Report RADC-TR-86-132, *Knowledge Based and Database System Integration: A Base Line for a Design Methodology*, Air Force Systems Command, 1986.

Ultrasystems, Defense and Space Systems, Inc.,"Dissemination System," Contract # GS-00K-86-ADJ0134, unpublished paper, 1987.

United States Marine Corps, *Fleet Marine Force Manual (FMFM), 2-1,* 1980.

Zytkow, J., and Erickson, M.D., "Tactical Manager in a Simulated Environment," *Methodologies for Intelligence Systems,* Eds: Zbigniew W. Ras and Maria Zemankova, North Holland, 1987.

INITIAL DISTRIBUTION LIST

No Copies

1. Defense Technical Information Center   2
   Cameron Station
   Alexandria, Virginia   22304-6145

2. Library, Code 0142   2
   Naval Postgraduate School
   Monterey, California   93943-5002

3. Commandant of the Marine Corps   1
   Code TE 06
   Headquarters, U.S. Marine Corps
   Washington, DC   20380-0001

4. Professor Tung X. Bui, Code 54Bd   1
   Department of Administrative Sciences
   Naval Postgraduate School
   Monterey, California   93943-5000

5. Professor Carl Jones, Code 74   1
   Department of Command, Control & Communications
   Naval Postgraduate School
   Monterey, California   93943-5000

6. Landing Force Training Command, Pacific   2
   Attn: Capt Gary McLean, USMC
   Naval Amphibious Base, Coronado
   San Diego, California   92155-5034